Identiteit misbruikt? Je staat er niet alleen voor

Onderzoek naar de dienstverlening aan (mogelijke) slachtoffers van identiteitsfraude en de juridische mogelijkheden voor compensatie

Rapport

In opdracht van
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Oktober 2015

BMC | onderzoek

Universiteit Leiden

Dit rapport is opgesteld door BMC Onderzoek en de Faculteit der Rechtsgeleerdheid van de Universiteit Leiden.

BMC Onderzoek:
dr. Ischa van Straaten
drs. Susan van Klaveren
drs. Adri van der Peet
drs. Tom Plat

Universiteit Leiden:
mr.dr. Michiel Tjepkema
mr.drs. Michael Verhulst
prof.mr. Tom Barkhuysen

Projectnummer: 107789
Correspondentienummer: DH-2210-4636

Dit onderzoek is uitgevoerd in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De verantwoordelijkheid voor de inhoud van het onderzoek berust bij de auteurs. De inhoud vormt niet per definitie een weergave van het standpunt van de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

Inhoudsopgave

Deel A: Managementsamenvatting

Deel A: Managementsamenvatting

Burgers die te maken krijgen met identiteitsfraude moeten volgens de Tweede Kamer worden geholpen met de afwikkeling hiervan. De laatste jaren zijn er stappen gezet in de (centrale) hulpverlening aan slachtoffers. Zo is bijvoorbeeld het Centraal Meldpunt Identiteitsfraude en -fouten (CMI) opgericht. Om inzicht te krijgen in de begeleiding van slachtoffers en eventuele verbetermogelijkheden daarbij, verzoekt de motie-Gesthuizen (26 643, nr. 338) de regering "*te onderzoeken welke verbeterpunten er mogelijk zijn ten aanzien van het compenseren van slachtoffers van fraude en het beleid ten aanzien van hulp bij fraude duidelijk te communiceren richting burgers*".

Opdracht

In opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft BMC Onderzoek op basis van een documentstudie en interviews het handelen van verschillende publieke en private organisaties ten aanzien van slachtoffers van identiteitsfraude in beeld gebracht (zie onderdeel B). Een juridische verkenning, uitgevoerd door de Universiteit Leiden, maakt tevens deel uit van het onderzoek. Op grond van een analyse van wettelijke kaders, wetenschappelijke literatuur en jurisprudentie heeft de Universiteit Leiden de voorwaarden en regels voor compensatie voor publieke en private organisatie vergeleken (zie onderdeel C).

Impact van ID-fraude

De beeldvorming over identiteitsfraude wordt gedomineerd door uitzonderlijke gevallen zoals de zaak Kowsoleea[1]. Dat blijkt uit de reacties van veel geïnterviewde partijen. In de meeste gevallen zijn de gevolgen minder ingrijpend dan in de zaak Kowsoleea. De schade blijft volgens schattingen in de meeste gevallen beperkt tot enkele tientallen tot honderden euro's. Het herstel kan wel veel tijd kosten, doordat het slachtoffer bijvoorbeeld aangifte moet doen, organisaties moet verzoeken de vervalste gegevens te corrigeren en/of een nieuw identiteitsbewijs moet aanvragen. Daarnaast is er emotionele schade: slachtoffers van identiteitsfraude kunnen zich op een vergelijkbare manier onveilig voelen als slachtoffers van geweldsdelicten.

Omvang van ID-fraude

Recente onderzoeken[2] schatten het aantal slachtoffers van identiteitsfraude jaarlijks op 1-5 procent van de volwassen Nederlandse bevolking.

[1] In deze zaak geeft Imro Cairo zich uit voor de zakenman Ron Kowsoleea. Vanaf dat moment worden de delicten van Cairo gekoppeld aan de naam Kowsoleea. Het duurt 19 jaar voordat de identiteit van de zakenman is hersteld.

[2] PWC, 2013; Paulissen en Van Wilsem, 2015.

Het grootste deel daarvan betreft skimming, phishing en pharming[3]. Andere vormen van identiteitsfraude, zoals fraude met identiteitsbewijzen en kopieën ervan, komen, met name volgens de uitvoeringsorganisaties, beduidend minder voor; al signaleert het CMI wel een toename in de bij haar *gemelde* zaken. De geraadpleegde organisaties geven aan dat zij identiteitsfraude niet afzonderlijk registreren.

Bij veel organisaties hogere drempels voor fraudeurs

Het onderzoek leert dat zowel publieke als private organisaties maatregelen hebben getroffen ter voorkoming van ID-fraude. In beide sectoren zien we dat beveiligingsfilters signalen van mogelijke fraude detecteren en dat wijzigingsprocedures (bijvoorbeeld van een rekeningnummer) zijn voorzien van extra controlemiddelen. Een aantal uitvoeringsorganisaties van de overheid is daarnaast overgegaan op een hoger beveiligingsniveau van DigiD.

Identiteitsfraude door kwetsbaarheden bij private organisaties

Bij de thuiswinkelsector komt identiteitsfraude vaak voor en wellicht ook in de telecomsector (er bestaat geen eenduidige beeld van deze sector). Ook (kleine) online banken die werken met afgeleide identificatie – waarbij een klein bedrag wordt overgemaakt vanaf een bestaande rekening bij een grote Nederlandse bank – lopen een verhoogd risico op identiteitsfraude en hun klanten evenzeer.

3 Skimming is het op onrechtmatige wijze bemachtigen en kopiëren van betaalkaartgegevens. Phishing is het oplichten van mensen door ze te lokken naar een valse (bank)website om ze daar te laten inloggen met hun inlognaam, wachtwoord en/of creditcardnummer. Hierdoor krijgt de fraudeur de beschikking over deze gegevens. **Pharming is** een oplichtingstechniek die erin bestaat internetgebruikers te misleiden door hun internetverkeer met een bepaalde website ongemerkt om te leiden naar een andere (malafide) website.

In de thuiswinkelsector maakt identiteitsvaststelling geen deel uit van het aankoopproces, maar wordt gecontroleerd aan de hand van het betaalmiddel. De aard van de dienstverlening brengt met zich mee dat deze sector zich genoodzaakt ziet identiteitsfraude als een bedrijfsrisico te zien en dit in hun verdienmodel te incalculeren. De dienstverlening van deze bedrijven is door een lager beveiligingsniveau (ook voor fraudeurs) makkelijker toegankelijk en ze zijn tegelijkertijd bereid de geleden schade te compenseren. Om fraude te voorkomen benoemt een aantal geïnterviewden van private organisaties de behoefte aan een overzicht/database met 'valse identiteiten'.

Fraude door kwetsbaarheden bij burgers/consumenten

Voordat ze over gaan tot compensatie checken publieke en private organisaties wat de rol van het slachtoffer zelf is geweest. Eerder onderzoek (PWC, 2013) wees uit dat de meeste Nederlanders maatregelen nemen om (bepaalde vormen van) identiteitsfraude te voorkomen. Ondanks de vele maatregelen komt identiteitsfraude nog voor. Redenen hiervoor kunnen zijn dat burgers wel maatregelen nemen, maar niet voldoende maatregelen om zich te wapenen tegen de verschillende (nieuwe) vormen van fraude. Daarnaast komt het voor dat burgers persoonlijke informatie delen in de familiaire sfeer (exen-fraude) of verstrekken aan personen die zich onterecht als werknemer presenteren van een bedrijf.

Begeleiding van slachtoffers door publieke en private organisaties

De meeste organisaties, zeker de uitvoeringsorganisaties van de overheid, besteden aandacht aan het begeleiden van slachtoffers. Dit blijkt uit het feit dat deze organisaties beschikken over een gespecialiseerde medewerker voor identiteitsfraude en/of een afdeling die het onderzoek uitvoert (en daarbij kijkt naar wat er is

voorgevallen en vaak het slachtoffer van advies voorziet). Zowel publieke als private organisaties adviseren slachtoffers aangifte bij de politie te doen om hen beter te kunnen helpen en omdat dan (extra) gecontroleerd wordt of een fraudeur zich als slachtoffer voordoet. Met name overheidsorganisaties verwijzen slachtoffers voor (extra) begeleiding vaak door naar het CMI; private partijen zijn minder bekend met het CMI.

CMI: centrale partij in begeleiding van slachtoffers

Het CMI is de voornaamste hulpverlenende instantie. Het CMI brengt de zaak samen met het slachtoffer in kaart, adviseert over te nemen stappen en bemiddelt richting (overheids)organisaties. Andere hulpverleners, zoals de Fraudehelpdesk en Slachtofferhulp Nederland, zijn minder gespecialiseerd in identiteitsfraude en verwijzen slachtoffers doorgaans door naar het CMI. Het CMI heeft een goed netwerk, vooral in de publieke sector, en werkt aan uitbreiding in de private sector.

Aangifte doen: nog verbeteringen nodig?

Publieke en private organisaties die aangifte bij de politie als voorwaarde stellen voor de hulp aan slachtoffers ervaren dat de mogelijkheid daartoe – identiteitsfraude is sinds mei 2014 als zelfstandig strafbaar feit opgenomen in het Wetboek van Strafrecht – nog niet in alle geledingen van de politie is doorgedrongen. De politie is inmiddels bezig met een intern opleidingstraject om hierin verbetering te brengen.

Na aangifte vaak compensatie van financiële schade

Als een slachtoffer aangifte heeft gedaan en (intern) onderzoek wijst uit dat het slachtoffer zelf niet verantwoordelijk is, herstellen de geïnterviewde publieke en private organisaties veelal de directe schade van de identiteitsfraude; zoals het alsnog uitkeren van studiefinanciering/uitkering of het stopzetten van een vordering. De schade die resteert nadat dergelijke gevolgen van de identiteitsfraude zijn hersteld (de zogenaamde gevolgschade), zoals de kosten van nieuwe identiteitsdocumenten, rechtsbijstand en of emotionele schade wordt in principe niet gecompenseerd. In de praktijk blijkt dat weinig slachtoffers hiervoor een verzoek tot compensatie doen.

Verschil in rechtsherstel tussen publieke en private sector

De bewijslast van identiteitsfraude verschilt per sector. In de publieke sector dragen burgers zelf de bewijslast om aannemelijk te maken dat zij slachtoffer zijn geworden van identiteitsfraude. Bestuursorganen mogen in beginsel uitgaan van de juistheid van de bij hen aangeleverde gegevens. De burger moet alert en proactief reageren vanaf het moment dat de fraude hem bekend kon zijn. In de private sector dient de private organisatie vaker te verklaren hoe hij de identiteit van de wederpartij heeft gecontroleerd. In geval van een rechtszaak wachten private partijen een rechterlijke uitspraak veelal niet af, maar gaan uit zichzelf over tot compensatie. Overheidspartijen focussen vooral op het ongedaan maken van de directe gevolgen van de identiteitsfraude. Een beroep op vergoeding van de gevolgschade wordt in de praktijk niet gedaan.

Herstel van registraties soms moeizaam bij gemeenten

Wijziging van gegevens in de basisregistratie personen, zoals deze worden geregistreerd door gemeenten, is met extra waarborgen omgeven en complex van aard om fraude te voorkomen. Herstelacties van identiteitsgegevens zijn daarom moeilijk. Het CMI geeft aan soms gemeenten te moeten ondersteunen bij het doorvoeren van de (juiste) wijziging in de basisregistratie.

De volgende stap

Het onderzoek levert een gemengd beeld op van de begeleiding van slachtoffers. Er zijn diverse organisaties, die de begeleiding van slachtoffers inmiddels naar eigen zeggen goed organiseren. Wat slachtoffers van die begeleiding vinden en of deze voldoende is, moet blijken uit het onderzoek onder slachtoffers dat de Belastingdienst parallel aan dit onderzoek uitvoert. De twee onderzoeken tezamen bieden inzicht in de (ervaren) knelpunten in de behandeling van slachtoffers van identiteitsfraude en kunnen zo opmaat zijn voor verbeterplannen.

Deel B: Onderzoek naar de dienstverlening aan (mogelijke) slachtoffers van identiteitsfraude

1. Inleiding

1.1 Aanleiding

Burgers die te maken krijgen met identiteitsfraude moeten volgens de Tweede Kamer goed worden geholpen met de afwikkeling hiervan. Dit om materiële en immateriële schade voor de slachtoffers te beperken en het vertrouwen van burgers in overheidssystemen te behouden en vergroten.

Naast burgers en bedrijfsleven, heeft de (centrale) overheid een verantwoordelijkheid in het tegengaan van identiteitsfraude. Deze vloeit voor de centrale overheid onder meer voort uit haar stelselverantwoordelijkheid voor de basisregistraties, de verstrekkende functie (toeslagen, uitkeringen, et cetera), de doelstellingen rondom het tegengaan van fraude met overheidsregelingen en de verantwoordelijkheid voor dienstverlening richting slachtoffers.

Er zijn de laatste jaren stappen gezet in de centrale hulpverlening aan slachtoffers, onder andere door de instelling van het Centraal Meldpunt Identiteitsfraude en -fouten (CMI). Ook is ingezet op monitoring van het fenomeen.[4] De volgende fase in de invulling van hulpverlening en afhandeling dient zich nu aan, mede door de motie-Gesthuizen (26 643, nr. 338). De motie verzoekt de regering "te onderzoeken welke verbeterpunten er mogelijk zijn ten aanzien van het compenseren van slachtoffers van fraude en het beleid ten aanzien van hulp bij fraude duidelijk te communiceren richting burgers".

Vergroten inzicht in afwikkeling identiteitsfraudezaken

Om als overheid de verantwoordelijkheid rondom hulpverlening beter te kunnen vervullen, is het noodzakelijk te weten op welke wijze organisaties (uitvoeringsdiensten van de overheid enerzijds en marktpartijen anderzijds) momenteel handelen als een slachtoffer van identiteitsfraude zich meldt. Het CMI is een belangrijke schakel in de hulpverlening, maar er zijn ook andere overheidsorganisaties en marktpartijen die delen in de verantwoordelijkheid voor het aanpakken van identiteitsfraude en het herstellen van de schade voor slachtoffers. Inzicht in de huidige hulpverlening en afhandeling, samen met het inzicht in de ervaringen van slachtoffers zelf, kan helpen bij het verbeteren van de hulpverlening.

Opdracht

In opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelatie heeft BMC Onderzoek in samenwerking met de Universiteit Leiden een onderzoek uitgevoerd waarmee het handelen van verschillende organisaties ten aanzien van slachtoffers van identiteitsfraude in beeld wordt gebracht. Dit onderzoek schetst een beeld vanuit het perspectief van de (geïnterviewde) organisaties. Hoe slachtoffers de geboden dienstverlening ervaren, komt in dit onderzoek enkel aan de orde via de hulpverlenende organisaties.

[4] Onder andere via de rapporten 'Omvang van identiteitsfraude & maatschappelijke schade in Nederland' door PWC (2011, update 2013) en 'Identiteit in cijfers' (Panteia, 2014).

Het perspectief van slachtoffers staat centraal in een onderzoek dat de Belastingdienst doet naar de beleving van slachtoffers[5]. Beide onderzoeken bieden tezamen een compleet beeld van ervaren schade, beleving van de hulp-/dienstverlening, de feitelijke maatregelen en wensen rondom de hulpverlening en compensatie.

1.2 Onderzoeksvragen

In het onderzoek staan de volgende drie hoofdvragen centraal.

1. Wat zijn de gevolgen voor slachtoffers van identiteitsfraude in verschillende situaties: bij verschillende werkwijzen van fraudeurs en in relatie tot verschillende organisaties waar fraudeurs hun slag slaan?
2. Welke obstakels vinden slachtoffers van identiteitsfraude op hun weg als zij de gevolgen van identiteitsfraude ongedaan willen maken en nieuwe gevolgen willen voorkomen?
3. Hoe worden slachtoffers van identiteitsfraude geholpen bij het herstel: door de overheid en in de financiële sector, in de telecomsector en in de thuiswinkelsector.

In verband met de schade en eventuele compensatie is het van belang te weten welke juridische mogelijkheden op het gebied van aansprakelijkstelling slachtoffers van identiteitsfraude ter beschikking staan en wat de verschillen tussen de private en publieke sector zijn.

Definitie en afbakening

De definitie van identiteitsfraude is aan veranderingen onderhevig en is afhankelijk van de reikwijdte van het bestudeerde fenomeen. In dit onderzoek is uitgegaan van de in 2014 geïntroduceerde definitie in het Wetboek van Strafrecht (Art 231b), omdat het de gevolgen voor het slachtoffer centraal stelt:
"Hij die opzettelijk en wederrechtelijk identificerende persoonsgegevens, niet zijnde biometrische persoonsgegevens, van een ander gebruikt met het oogmerk om zijn identiteit te verhelen of de identiteit van de ander te verhelen of misbruiken, waardoor uit dat gebruik enig nadeel kan ontstaan, wordt gestraft met […]"

Het gaat hier om een brede definitie, waarbij identificatiemiddelen kunnen bestaan uit identiteitsdocumenten (paspoort, NIK, rijbewijs, et cetera), authenticatiemiddelen (DigiD) of (PIN)passen in combinatie met codes die daders toegang geven tot middelen, diensten of producten van overheden of private partijen, ten koste van een ander[6].

Naast burgers kunnen ook bedrijven nadelige gevolgen ondervinden van identiteitsfraude. Dit onderzoek focust echter alleen op de gevolgen hiervan voor burgers.

1.3 Onderzoekverantwoording

Om de onderzoeksvragen te beantwoorden zijn door BMC Onderzoek de volgende activiteiten ondernomen. De verantwoording van de

juridische verkenning, uitgevoerd door de Universiteit Leiden, staat beschreven in hoofdstuk 7.

[5] Belastingdienst, 'Verkennend onderzoek context slachtoffers identiteitsfraude' (2015).

[6] Misbruik van biometrische persoonsgegevens is in het onderzoek niet aangetroffen.

A. Literatuurstudie

Om een eerste indruk te krijgen van het aantal slachtoffers van identiteitsfraude en de gemiddelde schadeomvang is relevante literatuur bestudeerd. De beschikbare bronnen zijn systematisch langs de onderzoeksvragen gelegd. In bijlage B is een lijst van gebruikte bronnen opgenomen.

B. Interviews

Voor het onderzoek hebben we een aantal organisaties geïnterviewd over het thema identiteitsfraude, verdeeld naar publieke en private organisaties. De deelnamebereidheid bleek in sommige onderdelen van de private sector tegen te vallen. Met name in de telecomsector en in de e-commerce was het lastig om gesprekspartners te vinden. Om uiteindelijk tot het huidige aantal interviews te komen, zijn enkele tientallen andere organisaties benaderd.

Tabel 1 bevat een overzicht van categorieën van organisaties en aantallen interviews per categorie. In bijlage C is een overzicht opgenomen van alle geïnterviewde organisaties.

Tabel 1 Overzicht van bevraagde organisaties

Organisatie	Aantal interviews
Hulpverlenende instanties overheid	3
Hulpverlenende instantie privaat	2
Uitvoeringsorganisaties overheid	12
Gemeenten	9
Financiële sector	4
Telecomsector	3
Thuiswinkelbranche	6
Overig	4
Totaal	**43**

Voor zowel de publieke als de private sector geldt dat het aantal afgenomen interviews niet voldoende is om een representatief beeld voor de gehele sector te schetsen. De uitkomsten van deze interviews, zoals beschreven in de hoofdstukken 3, 4 en 5, dienen dan ook met enige voorzichtigheid te worden gelezen.

De interviews zijn voor het grootste deel persoonlijk afgenomen, waarbij in de meeste gevallen meerdere functionarissen van de organisatie aanwezig waren. De benodigde informatie uit de bancaire wereld is verkregen tijdens een groepsbijeenkomst die de Nederlandse Vereniging van Banken (NVB) voor ons had belegd.

In overleg met de begeleidingscommissie zijn de te bespreken thema's/vragen benoemd. Per organisatie is vervolgens een checklist gemaakt met alle voor die organisatie relevante onderwerpen. De duur van de interviews en de mate van verdieping verschilt tussen de respondenten en is vooral afhankelijk van de mate waarin de organisatie fraudegevallen registreert en maatregelen treft om fraude tegen te gaan.

C. Uitvraag onder zorgverzekeraars

Met behulp van Zorgverzekeraars Nederland is een vragenlijst uitgezet onder de fraude-afdelingen van de zorgverzekeraars. Twee grote en twee kleinere zorgverzekeraars hebben de vragen beantwoord, waarna een medewerker van het Kenniscentrum Fraudebeheersing van de koepelorganisatie de antwoorden heeft samengevat. De reacties zijn in dit rapport op dezelfde manier verwerkt als de interviews.

D. Bespreking en verificatie rapportage

Conceptversies van deze rapportage zijn besproken met de begeleidingscommissie en tevens voorgelegd aan de geïnterviewde partijen, om feitelijke onjuistheden te kunnen corrigeren.

1.4 Leeswijzer

Hoofdstuk 2 geeft inzicht in de aard en omvang van identiteitsfraude. De verschillende vormen van identiteitsfraude worden behandeld en er wordt inzicht gegeven in de aantallen slachtoffers. Ook wordt een beeld geschetst van de gemiddelde schadeomvang.

Hoofdstuk 3 gaat in op waar slachtoffers zich melden wanneer zij door hebben dat zij slachtoffer zijn geworden van identiteitsfraude.

Hoofdstuk 4 en 5 behandelen de wijze waarop respectievelijk publieke en private organisaties meldingen van identiteitsfraude afwikkelen.

Hoofdstuk 6 tot slot behandelt de wijze waarop politie en hulpverlenende organisaties omgaan met identiteitsfraude. Dit hoofdstuk sluit af met informatie over schadefondsen.

Hoofdstuk 7, onderdeel C, beschrijft de juridische verkenning waarin de mogelijkheden van compensatie van slachtoffers van identiteitsfraude is onderzocht.

2. Identiteitsfraude in cijfers

Voordat we ingaan op de wijze waarop organisaties meldingen van identiteitsfraude behandelen, schetst dit hoofdstuk een beeld van de aard en omvang van identiteitsfraude en de bijbehorende schadelast. De eerste paragraaf behandelt de verschillende modi operandi waar het gaat om identiteitsfraude. Paragraaf 2 gaat in op de prevalentie van identiteitsfraude en paragraaf 3 behandelt de aard van de fraude. De vierde paragraaf schetst de schade als gevolg van identiteitsfraude.

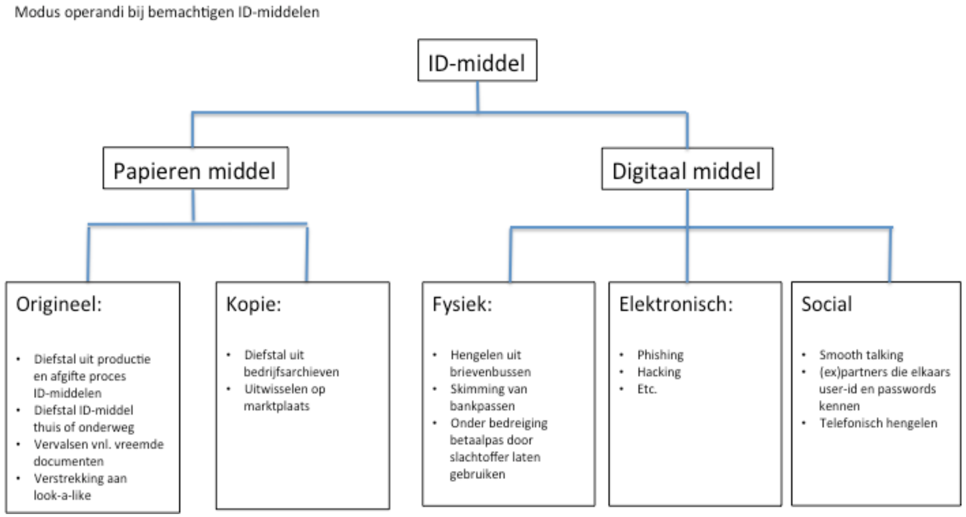
Bij dit hoofdstuk is een kanttekening op zijn plaats. Er zijn verschillende onderzoeken naar het aantal slachtoffers van ID-fraude uitgevoerd. Op grond van deze onderzoeken is het niet mogelijk om een eenduidig beeld te schetsen van de prevalentie van identiteitsfraude en de daardoor geleden schade. De onderzoeken hanteren namelijk verschillende definities van identiteitsfraude, beslaan verschillende tijdsbestekken en gebruiken verschillende onderzoeksmethoden. Waar nodig worden deze verschillen in de navolgende paragrafen benoemd.

2.1 Modi operandi

Het delict identiteitsfraude vindt in twee stappen plaats. Allereerst dient de (aanstaande) dader de identiteitsdocumenten en/of gegevens van het slachtoffer te verkrijgen (door diefstal, kopen of anderszins). Het gaat hierbij zowel om het verkrijgen van de fysieke documenten of een kopie daarvan, als het digitaal verkrijgen van persoonlijke gegevens. Wanneer de dader deze in handen heeft, kan hij/zij met de verkregen persoonlijke informatie frauderen.

Figuur 2.1 toont de verschillende vormen van identiteitsfraude. Het gaat hier om mogelijke verschijningsvormen, omdat de prevalentie niet van alle *modi operandi* bekend is.

Figuur 2.1 Modi operandi bemachtigen ID-middelen



Bron: Paulissen en Van Wilsem, 2015

Uit de figuur blijkt dat identiteitsfraude op zeer uiteenlopende manieren kan worden gepleegd. Dit varieert van relatief simpele varianten zoals post hengelen tot complexe varianten waarin sprake is van een taakverdeling tussen hackers, tussenpersonen die op illegale online marktplaatsen de gestolen persoonsgegevens verhandelen, ‘katvangers’ die hun bankrekening ter beschikking stellen, en de initiator van het geheel. Belangrijk is om vast te houden dat identiteitsfraude geen doel op zich is; het is een middel, een modus operandi, om een ander delict te plegen en op die manier financieel dan wel crimineel gewin te behalen.

2.2 Aantallen slachtoffers

Deze paragraaf behandelt de prevalentie van identiteitsfraude aan de hand van een aantal onderzoeken.

In de update van het onderzoek '*Omvang van identiteitsfraude en de maatschappelijke schade in Nederland*' stelt PWC op basis van een online enquête onder een panel (ingevuld door ruim 5.000 respondenten) en een gewogen schatting dat het aantal (volwassen) slachtoffers van ID-fraude in 2012 612.000 bedraagt[7]. PWC gaat hierbij uit van een betrouwbaarheidsinterval tussen de 532.000 en 706.000 burgers. De definitie van ID-fraude die PWC in het onderzoek heeft gehanteerd is zeer breed en omvat naast misbruik van (kopieën van) identificatiedocumenten ook digitale fraudevormen, zoals skimming, phishing en pharming[8].

Tabel 2.1 Slachtoffers van identiteitsfraude

	Percentage	
	%	***95% BI*[B]**
Slachtoffer ooit	16,3	*15,9/18,4*
Slachtoffer 2007-2012	13,2	*12,8/15,1*
Slachtoffer in 2012	4,6	*4,0/5,2*
N	5.039	

Bron: PWC (2013)

Op basis van een enquête schatten de auteurs dat circa 16,3% van de volwassen Nederlandse bevolking *ooit* slachtoffer is geweest en dat 13,2% van de bevolking *in de jaren 2007 tot en met 2012* slachtoffer van identiteitsfraude is geweest. De auteurs geven evenwel aan dat dit nogal ruwe schattingen zijn.

In het recent gepubliceerd rapport '*Dat heeft iemand anders gedaan!*' (Paulissen en Van Wilsem, 2015) in opdracht van Politie en Wetenschap is onderzocht hoe groot de prevalentie is onder een panel van ruim 5.000 respondenten[9]. Paulissen en Van Wilsem definiëren identiteitsfraude als onrechtmatige bankafschrijvingen (bankfraude), misbruik van creditcards en misbruik van persoonlijke informatie (overige fraude). De totale prevalentie is zowel voor de periode 2008-2010 als voor 2010-2012 4,6%[10].

Tabel 2.2 Percentage slachtofferschap [A]

	2008-2010		2010-2012	
	%	***95% BI*[B]**	**%**	***95% BI***
Bankfraude	3,6	*3,1/4,1*	3,5	*3,0/4,0*
Creditcardfraude	1,0	*0,7/1,2*	0,9	*0,7/1,2*
Overige fraude	0,3	*0,2/0,4*	0,4	*0,2/0,6*
Totaal	4,6	*4,1/5,2*	4,6	*4,0/5,1*
N	5.764		5709	

Bron: Paulissen en Van Wilsem (2015)

[A] Gewogen op basis van geslacht, leeftijd, opleidingsniveau en urbanisatiegraad

[B] 95%-betrouwbaarheidsintervallen: de ondergrens en de bovengrens zijn hierbij aangegeven

---

[7] PWC, 2013-update onderzoek 'Omvang van identiteitsfraude & maatschappelijke schade in Nederland (Amsterdam, mei 2013).

[8] PWC hanteert de definitie uit de WODC-studie 'Identiteitsfraude: een afbakening, een internationale begripsvergelijking en analyse van nationale strafbepalingen': *'Identiteitsfraude is het opzettelijk (en) (wederrechtelijk of zonder toestemming) verkrijgen, toe-eigenen, bezitten of creëren van valse identificatiemiddelen en het daarmee begaan van een wederrechtelijke gedraging of: met de intentie om daarmee een wederrechtelijke gedraging te begaan'*

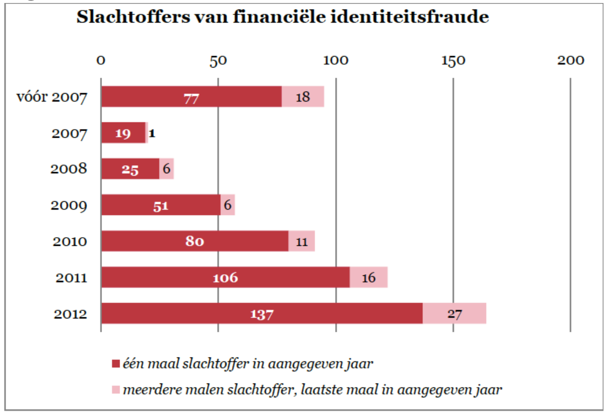
[9] Hierbij is gebruikgemaakt van het LISS-panel, waaraan mensen uit alle lagen van de Nederlandse bevolking deelnemen. Zij vullen via internet vragenlijsten in. Paulissen en Van Wilsem hebben vragen toegevoegd aan de enquêtes van februari 2010 en 2012 jaar over identiteitsfraude in de 2 jaar voorafgaand aan de enquête.

[10] 'Dat heeft iemand anders gedaan! Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland (PW82)' Door: L. Paulissen, J.A. van Wilsem, Politiewetenschap 82, Politie en Wetenschap, Apeldoorn; Reed Business, Amsterdam 2015.

PWC en Paulissen en Van Wilsem laten een gelijk percentage zien: 4,6% in 2012 volgens PWC en Paulissen en Van Wilsem over de periode 2010-2012. Er zijn echter twee verschillen.
Het onderzoek van PWC betreft één kalenderjaar terwijl het onderzoek van Paulissen en Van Wilsem twee kalenderjaren beslaat. Ook kijken Paulissen en Van Wilsem wel naar gevolgen van identiteitsfraude door onrechtmatige bankafschrijvingen, misbruik van creditcards en andere ID-fraudevormen, maar niet naar de wijze waarop de fraude is gepleegd. Identiteitsdiefstal en het creëren van valse identificatiemiddelen blijven buiten beschouwing.

In de update van het onderzoek '*Omvang van identiteitsfraude en de maatschappelijke schade in Nederland*' constateert PWC in 2013 echter dat financiële identiteitsfraude sinds 2007 jaar op jaar toeneemt. Onder financiële identiteitsfraude verstaat PWC het skimmen van een pinpas, automatische incasso's op andermans naam, diefstal van creditcardgegevens, aankoop van spullen op naam van slachtoffer, huren van een voertuig of spullen met gebruik van (een kopie van) het paspoort van een slachtoffer.

Figuur 2.2 Slachtoffers van financiële identiteitsfraude



Bron: PWC, 2013

De *Veiligheidsmonitor* van het CBS focust op online identiteitsfraude in de financiële sector, waarbij private identificatiemiddelen (bankpassen, creditcards, gebruikersgegevens) worden misbruikt om oneigenlijke toegang te krijgen. Net als het onderzoek van Paulissen en Van Wilsem tonen de CBS-cijfers een daling van de fraude in de financiële sector.

Tabel 2.3 Slachtoffers financieel economische identiteitsfraude per 100 inwoners

	2012	**2013**
Skimming	1,1	0,8
Phishing/pharming	0,5	0,5
Hacking, ingebroken op computer	1,5	1,5
Hacking, ingebroken op email account	3,9	3,5
Hacking, ingebroken op website	2,2	2,5
Hacking, anders	3,3	2,7

Bron: Criminaliteitsstatistiek, CBS

Naast 'skimming' en 'phishing/pharming' richt het CBS-onderzoek zich ook koop- en verkoopfraude, omdat identiteitsfraude hier onderdeel van kan uitmaken[11]. In 2014 is 3,5 procent van de Nederlanders slachtoffer geweest van koop- en verkoopfraude. Dit is hoger dan in 2012 toen dit 2,9 procent was maar vergelijkbaar met 2013 (3,3 procent). De toename wordt veroorzaakt door de stijging van koopfraude.

Dezelfde daling zien we terug in de cijfers van de *Nederlandse Vereniging van Banken (NVB)*. Zowel qua skimming als fraude met internetbankieren gaat het om een sterke daling.

Tabel 2.4 Identiteitsfraude zoals gerapporteerd door de NVB

	2012	**2013**
Aantal geskimde passen	51.200	11.000
Fraude met internetbankieren (geslaagde pogingen)	10.900	3.500

Bron: Nederlandse Vereniging van Banken (Panteia, 2014)

Naast identiteitsfraude met de identificatiemiddelen zelf, kan in de financiële sector ook fraude plaatsvinden door 'afgeleide identificatie'. Hierbij kunnen fraudeurs rekeningen openen of leningen afsluiten op naam van iemand anders. Er zijn echter geen cijfers bekend over hoe vaak identiteitsfraude voorkomt bij afgeleide identificatie[12].

Het *Expertisecentrum Identiteitsfraude en -documenten (ECID)* heeft daarnaast cijfers van fraude met Nederlandse identiteitsdocumenten of kopieën daarvan. Tussen 2012 en 2013 nam het aantal gevallen met originele documenten in Nederland toe, maar daalde het aantal incidenten in het buitenland.

Tabel 2.5 Fraude met Nederlandse documenten

		2012	**2013**
In Nederland[13]	Geconstateerde gevallen van fraude met originele documenten	76	104
	Geconstateerde gevallen van fraude met kopieën	233	231
In het buitenland (België, Duitsland en VK)	Aantal zaken van European Document Fraud Analysis Network	122	97

Bron: ECID, bewerking Panteia, 2014

Op grond van het voorgaande is het lastig om eenduidig vast te stellen wat de prevalentie van identiteitsfraude is. Het onderzoek van PWC (2013) komt op een prevalentie van 4,6%. Ditzelfde percentage ziet Paulissen en Van Wilsem over een periode van twee jaar. Dit duidt op een iets lagere prevalentie dan het PWC-onderzoek. Skimming, phishing en pharming, wat het merendeel is van identiteitsfraude, is volgens CBS ruim 1%. Op grond hiervan stellen we dat het aantal slachtoffers van identiteitsfraude in 2013 neerkomt op 1-5% van de volwassen Nederlandse bevolking.

2.3 Verdeling naar aard

Naast de prevalentie behandelen meerdere onderzoeken hoe de verschillende vormen van identiteitsfraude zich tot elkaar verhouden.

[11] Centraal Bureau voor de Statistiek, 'Veiligheidsmonitor' (Den Haag, 2014, p75)

[12] Identiteit in cijfers, Panteia, 2014, pag. 26.

[13] Berekening Panteia op basis van meer gedetailleerde gegevens van ECID, gepubliceerd in 'Identiteit in cijfers 2014'.

In de update van het onderzoek '*Omvang van identiteitsfraude en de maatschappelijke schade in Nederland*' (PWC, 2013) toont PWC dat financiële fraude met 46% het meeste voorkomt. De volgende tabel toont de percentuele verdeling naar fraudevorm op basis van een uitvraag onder respondenten die ooit slachtoffer zijn geworden van identiteitsfraude (16%)[14].

Tabel 2.6 Vormen van identiteitsfraude

Vorm	**%**
Financiële fraude	46%
Fraude via het internet	18%
Criminele fraude	11%
Medische fraude	9%
Overige fraude	15%

Bron: PWC, 2013

Het rapport '*Dat heeft iemand anders gedaan!*' (Paulissen en Van Wilsem, 2015) laat eveneens zien dat slachtoffers vooral getroffen worden door financiële fraude. Meer dan 70% van de slachtoffers heeft te maken gekregen met bankfraude (onrechtmatige bankafschrijvingen). Het aandeel creditcardfraude schommelde rond de 20%, de overige vormen van fraude (waaronder medische fraude en het aanvragen van een financieel product) betrof 6 à 7%. De cijfers tonen een lichte daling in zowel bank- als creditcardfraude. Net als bij de cijfers van PWC geeft de tabel een indicatief beeld, daar de uitkomsten zijn gebaseerd op een klein aantal slachtoffers (4,6% van alle respondenten).

[14] Respondenten hebben meerdere vormen kunnen aangeven. In totaal melden de 833 respondenten slachtoffer te zijn geweest van 1.265 vormen.

Tabel 2.7 Aard van de identiteitsfraude

	2008-2010	**2010-2012**
Bankfraude	74,2%	71,7%
Creditcardfraude	19,6%	21,2%
Overige fraude	6,2%	7,2%
Totaal	100%	100%
N	260	265

Bron: Paulissen en Van Wilsem (2015)

2.4 Omvang van de schade

Slachtoffers van identiteitsfraude kunnen omvangrijke schade lijden doordat hun identiteit is misbruikt. De schadevorm die de meeste aandacht krijgt, is doorgaans de directe financiële schade. Bijvoorbeeld hoeveel iemand heeft verloren toen de bankrekening werd geplunderd of wat er is aangeschaft op zijn naam.

2.4.1 Directe financiële schade

Totale financiële schadeomvang

De update van het onderzoek '*Omvang van identiteitsfraude en de maatschappelijke schade in Nederland*' (PWC, 2013) gaat op basis van een relatief klein aantal slachtoffers in op de (geschatte) totale omvang van het schadebedrag als gevolg van identiteitsfraude. Na een toename tussen 2007 en 2010 daalt de omvang van de geleden schade in de jaren 2011 en 2012, ondanks dat het totale aantal slachtoffers in deze periode is toegenomen.

Tabel 2.8 Geschatte schadeomvang, bedragen afgerond en gepresenteerd in miljoenen euro's

	2007	2008	2009	2010	2011	2012
Schade	63	395	697	736	544	355
95% ondergrens	-	-	-	192	171	207
95% bovengrens	-	-	-	1279	918	504

Bron: PWC, 2013

In het rapport '*Dat heeft iemand anders gedaan!*' (Paulissen en Van Wilsem, 2015) zijn de resultaten voor onrechtmatige bankafschrijvingen voor de schatting geëxtrapoleerd naar het bevolkingsaantal in de twee perioden. Voor de periode 2008-2010 ligt de geschatte directe financiële schade, gezien de prevalentie van 3,6% slachtofferschap, tussen de € 147 en € 248 miljoen. Voor 2010 tot 2012 komt de schatting uit op een bedrag tussen de € 134 en € 228 miljoen.

Als gevolg van de daling in het aantal geskimde passen en fraude met internetbankieren, daalt ook de schadepost van deze twee vormen van identiteitsfraude sterk.

Tabel 2.9 Identiteitsfraude zoals gerapporteerd door de NVB

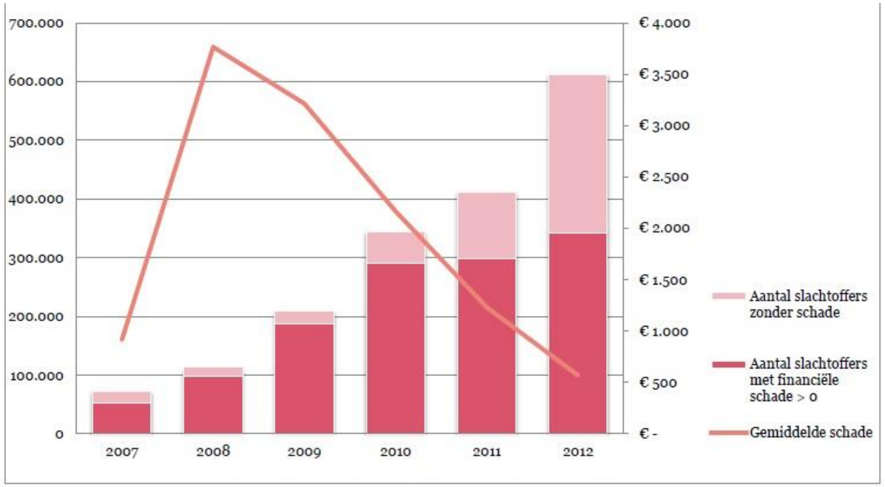
	2012	2013	2014
Schade van skimming	€ 28.900.000	€ 6.800.000	
Schade van fraude met internetbankieren	€ 34.800.000	€ 9.600.000	

Bron: Nederlandse Vereniging van Banken

Gemiddelde schadebedrag

Uit het onderzoek van PWC (2013) blijkt dat het gemiddelde schadebedrag in de periode 2007 tot en met 2012 bijna € 1.500 bedraagt. Na een piek van het gemiddelde schadebedrag in 2008 (bijna € 4.000) is dit bedrag gedaald tot ongeveer € 600 per schadegeval. PWC stelt dat hoewel het totale aantal slachtoffers tussen 2010 en 2012 is toegenomen de totale geschatte schade, als gevolg van de daling van het gemiddelde schadebedrag, is afgenomen.

Figuur 2.3 Schatting aantal slachtoffers en gemiddeld schadebedrag



Bron: PWC, 2013-update onderzoek 'Omvang van identiteitsfraude & maatschappelijke schade in Nederland.

In het rapport '*Dat heeft iemand anders gedaan!*' (Paulissen en Van Wilsem, 2015) wordt ook de schade beschreven die slachtoffers van

identiteitsfraude hebben ondervonden. Voor de perioden 2008-2010 en 2010-2012 geven zij aan dat de slachtoffers gemiddeld ongeveer € 407 en € 382 *bruto* schade ondervinden. Dit gemiddelde wordt, net als bij het onderzoek van PWC het geval is, voor een groot deel bepaald door een aantal uitschieters, ofwel hoge bedragen. De mediaan, die minder gevoelig is voor uitschieters, ligt op respectievelijk € 75 en € 100. Dat wil zeggen dat de helft van de slachtoffers meer schade heeft. De *netto* schade (na compensatie) is met gemiddeld respectievelijk € 25 en € 45 beduidend lager.

Een andere bron voor de gemiddelde schadelast zijn de meldingen bij het CMI (zie verder hoofdstuk 3). Het gemiddelde schadebedrag van meldingen bij het CMI bedraagt tussen 2011 en 2012 € 6.273. Dit gemiddelde is berekend op basis van 161 meldingen, waarbij 130 keer een schadebedrag groter dan € 0 is vermeld. Ruim de helft van de gemelde schadebedragen ligt onder de € 1.000, de rest ligt erboven[15].
In het rapport 'Omvang van identiteitsfraude & maatschappelijke schade in Nederland' stelt PWC dat het gemiddelde schadebedrag over een jaar eerder (de periode 1 maart 2010 tot 1 maart 2011) € 8.800 is. In tegenstelling tot de analyse over de periode 2011-2012 heeft PWC in deze analyse alleen de meldingen van burgers die aangaven schade te hebben geleden (53% van de meldingen)[16]. In de update van het onderzoek stelt PWC dat de daling in het gemiddelde schadebedrag overeenkomt met de trend die PWC in haar enquête onder burgers in 2012 vaststelt[17].
Het gemiddelde schadebedrag op grond van de CMI-meldingen is veel hoger dan zowel PWC als Paulissen en Van Wilsem vaststellen op basis van hun enquête onder burgers. Een mogelijke verklaring hiervoor is dat het CMI een 'tweedelijnsmeldpunt' is waar slachtoffers alleen terechtkunnen als zij niet tot overeenstemming komen met de organisatie waar de fraude heeft plaatsgevonden. Dit kan ertoe leiden dat het CMI vooral meldingen krijgt van zaken die complexer en/of omvangrijker van aard zijn.
Ditzelfde beeld zien we terug bij de politie. Paulissen en Van Wilsem (2015) noteren een aanzienlijk hoger gemiddeld schadebedrag bij slachtoffers die aangifte hebben gedaan ten opzichte van de niet-aangevers. Deze bedragen zijn voor de periode 2010-2012 respectievelijk circa € 1.300 versus € 250.

Schadevergoeding

Onderzoek van Paulissen en Van Wilsem toont dat vier op de vijf slachtoffers van identiteitsfraude in de perioden 2008-2010 en 2010-2012 de financiële schade vergoed hebben gekregen[18]. Circa 15% kreeg geen vergoeding, het resterende deel kreeg de schade deels vergoed. In het onderzoek van PWC (2013) geeft slechts 33% van de slachtoffers aan een schadevergoeding of compensatie te hebben gekregen.

2.4.2 Immateriële schade

In de update van het onderzoek 'Omvang van identiteitsfraude & maatschappelijke schade' (2013) meldt PWC dat 102 van de 356

[15] Er zijn twee uitschieters: een schadebedrag van € 5 miljoen en een schadebedrag van € 200.000. Eerstgenoemde is niet meegenomen in de berekening van het gemiddelde schadebedrag, het tweede schadebedrag wel.

[16] PWC, Centraal Meld- en Informatiepunt Identiteitsfraude en –fouten – Analyse van meldingen 2011-2012 (Amsterdam, april 2013).

[17] PWC, 2013-update onderzoek 'Omvang van identiteitsfraude & maatschappelijke schade in Nederland (Amsterdam, mei 2013).

[18] Paulissen en Van Wilsem, Dat heeft iemand anders gedaan! (Leiden, 2015).

respondenten die zeggen ooit slachtoffer te zijn geweest, geen financiële schade hebben geleden. Dit betekent niet dat de identiteitsfraude voor hen geen consequenties heeft gehad. Uit de interviews blijkt dat naast financiële schade slachtoffers ook immateriële schade ondervinden. Hierbij denken we aan zaken als spanning en frustratie bij mensen die, soms jarenlang, tegen hun wil verwikkeld raken in procedures om de fraude ongedaan te krijgen. Het bijhouden van een dossier en het steeds maar komen opdraven bij bepaalde instanties kost slachtoffers ontzettend veel tijd. Andere zaken zoals geregistreerd staan op één van de 'zwarte lijsten' in de private sectoren van bijvoorbeeld het Bureau Krediet Registratie (BKR) of Preventel (de zwarte lijst die de Nederlandse telecombedrijven gebruiken) kan tot schade leiden. Personen met een betalingsachterstand worden op zo'n lijst geplaatst, waardoor zij bepaalde diensten of producten niet meer kunnen aanschaffen. Het is evident dat het niet meer kunnen bellen met een mobiel het leven van het slachtoffer niet gemakkelijker maakt. Maar ook een onterechte aantekening bij Justitie kan indirect tot problemen leiden, bijvoorbeeld wanneer iemand aangehouden wordt door de politie, op Schiphol, of bij het aanvragen van een verklaring omtrent goed gedrag.

De meeste geïnterviewde publieke en private organisaties kunnen zich voorstellen dat de immateriële schade voor slachtoffers als gevolg van identiteitsfraude immens kan zijn. Men toont zich bewust van de impact die ID-fraude op een slachtoffer kan hebben. Goed beschouwd blijft immateriële schade subjectief en is het voor ieder slachtoffer anders. Het vertalen van de schade in euro's of compensatie is dan ook niet mogelijk.

2.5 Conclusie

Over identiteitsfraude doen tal van cijfers de ronde. Op grond van de beschreven onderzoeken ontstaat het volgende beeld:

- Tussen de 1% en 5% van de Nederlandse bevolking wordt per jaar slachtoffer van identiteitsfraude in brede zin.
- Skimming, phishing en pharming vormen daarbij het grootste aandeel, maar nemen wel af. Koopfraude, waar identiteitsfraude onderdeel van kan uitmaken, neemt daarentegen toe.
- Bij identiteitsfraude kan de schadeomvang per incident sterk verschillen. Sommige slachtoffers leiden enorme verliezen terwijl andere slachtoffers geen directe financiële schade hebben.
- Uit onderzoek onder een relatief klein aantal slachtoffers blijkt dat de gemiddelde schadelast enkele honderden euro's is.

Een betere registratie van identiteitsfraude, nu veelal ontbrekend, kan het inzicht in de prevalentie, aard en omvang van identiteitsfraude vergroten.

3. Meldingen van identiteitsfraude

Slachtoffers van identiteitsfraude kunnen zich op verschillende plaatsen melden, bijvoorbeeld bij de politie, bij meldpunten, bij slachtofferhulp. Volgens de geïnterviewde organisaties melden slachtoffers zich in eerste instantie vaak bij de partij waar het slachtoffer de gevolgen van de identiteitsfraude ondervindt. Dit hoofdstuk gaat respectievelijk in op meldingen bij uitvoeringsorganisaties, gemeenten, private organisatie, politie en meldpunten/hulpverleningsorganisaties.

3.1 Uitvoeringsorganisaties

Weinig zaken identiteitsfraude

De grote uitvoeringsorganisaties geven allemaal aan signalen te krijgen van identiteitsfraude. Naast directe meldingen van burgers bestaan er interne signalen op basis van controles en detectiesystemen, waarbij alarmsignalen afgaan als twijfelachtige mutaties zijn doorgevoerd of verdachte aanvragen zijn gedaan. Daarnaast ontvangen uitvoeringsorganisaties ook signalen via Logius (zie verder).

In de afgelopen jaren zijn er bij uitvoeringsorganisaties enkele honderden gevallen bekend, die grotendeels te herleiden zijn naar een beperkt aantal grootschalige fraudezaken met meerdere slachtoffers (zie kader).

Grootschalige fraudegevallen met DigiD

In 2013 en 2014 zijn enkele grootschalige incidenten geweest waarbij DigiD's zijn ontvreemd en gebruikt door derden.

- In 2013 hebben 90 Groningse studenten aangifte gedaan omdat brieven met DigiD inlogcodes uit de brievenbus zijn gehengeld. De daders hebben voor de slachtoffers nieuwe DigiD inlogcodes aangevraagd en daarmee onder andere zorg- en huurtoeslagen aangevraagd. De schade bedroeg volgens de recherche enkele tonnen. De slachtoffers zijn uiteindelijk allemaal schadeloos gesteld.
- Bij de 'Roosendaal-zaak' hebben daders via phishing inloggegevens van circa 180 DigiD's verkregen en deze gebruikt om gegevens op websites van overheidsorganisaties te wijzigen. De omvang van de fraude wordt geschat op circa € 50.000. De schade is relatief beperkt gebleven vanwege snelle reactie van de gezamenlijke overheidsdiensten. Logius heeft op 15 september aangifte gedaan bij de politie, mede namens het UWV en de SVB. De mensen die zijn getroffen, zijn schadeloos gesteld door de betrokken overheidsorganisaties. Logius heeft de 5.000 DigiD's verwijderd zodat er geen misbruik meer kon plaatsvinden en de betrokken burgers een brief gestuurd.

Bron: www.om.nl

Hieronder volgt per uitvoeringsorganisatie inzicht in de mate waarin identiteitsfraude binnen hun organisatie voorkomt.

- De Belastingdienst heeft te maken met enkele tientallen casussen per jaar. Een deel daarvan bestaat uit de zogenaamde exenfraude, waarbij exen over elkaars persoonlijke gegevens beschikken en doen voorkomen dat de ander daar

identiteitsfraude mee plegen. In het interview merkt de Belastingdienst op dat het bij identiteitsfraude om ‘zeldzaamheden’ gaat.

- De Dienst Uitvoering Onderwijs (DUO) heeft ongeveer vijf keer per jaar te maken met identiteitsfraude. Het gaat dan om studiefinanciering die is gestort op de bankrekening van de dader in plaats van het slachtoffer.
- Bij de KvK, waar fraudeurs met een kopie van een identiteitsbewijs wijzigingen van bedrijfsgegevens kunnen laten doorvoeren, wordt een aantal keer per jaar een ID-bewijs aangetroffen dat in het VIS (Verificatie Informatie Systeem van Bureau Krediet Registratie) geregistreerd staat. In deze gevallen wordt de gevraagde wijziging niet doorgevoerd.
- De RDW heeft te maken met twee vormen van identiteitsfraude. Fraude met rijbewijzen komt volgens de dienst slechts een enkele keer voor. Wel krijgt de dienst ongeveer twintig meldingen van fraude met kopieën van rijbewijzen. Daarnaast bestaat er fraude door onterechte tenaamstelling van voertuigen. De RDW krijgt circa 5.000 meldingen/bezwaren van een onterechte tenaamstelling. Slechts een klein deel hiervan is (juridisch gezien) terecht (drie keer in de afgelopen vijf jaar).
- De Sociale Verzekeringsbank (SVB) heeft vooral te maken met wijzigingen in bankrekeningnummers waardoor uitkeringen aan de verkeerde persoon worden uitbetaald. In 2013 en 2014 zijn er incidenten geweest waarbij meerdere klanten slachtoffer werden. In 2015 heeft de SVB geen signalen meer gekregen van dergelijke grootschalige fraudegevallen en is er vooral sprake van familiaire en exen fraude. De SVB heeft geen cijfers over hoe vaak de organisatie te maken heeft met (vermoedens van) identiteitsfraude.
- De Uitvoeringsinstituut Werknemersuitkeringen (UWV) kan te maken hebben met het verkrijgen van een uitkering met behulp van een vals of vervalst identiteitsbewijs en het verkrijgen van een uitkering op basis van rechten die door een ander zijn opgebouwd. In de praktijk komt dit door ingebouwde veiligheidsmaatregelen vrijwel niet meer voor.

RDW: veel onterechte meldingen van tenaamstelling

Bij de RDW is het aantal (onterechte) meldingen van fraude hoog. Om die reden worden meldingen direct gecontroleerd door de afdeling die bezwaren dan wel meldingen van onterechte tenaamstellingen beoordeelt. Deze afdeling handelt het leeuwendeel van de meldingen af als ongegrond, wat bewezen wordt via het nagaan van de historie van het voertuig in de verschillende registraties. Zo kan men bijvoorbeeld zien met welk identiteitsbewijs de kentekenregistratie heeft plaatsgevonden en of er boetes zijn betaald door de betreffende burgers. In slechts een handvol gevallen was er in de laatste jaren sprake van bewezen identiteitsfraude. Deze meldingen worden doorgezet naar de afdeling die zich met identiteitsfraude bezig houdt.

Bron: Interview RDW

Minder slachtoffers door hoger beveiligingsniveau

Een aantal uitvoeringsorganisaties, zoals de SVB, merken expliciet op dat het aantal gevallen van identiteitsfraude de afgelopen jaren is afgenomen. Bij de (enkele) incidenten van identiteitsfraude die zich hebben voorgedaan, is er sprake geweest van een grotere groep slachtoffers. Aangezien uitvoeringsorganisaties relatief lage bedragen uitkeren, is het voor de fraudeur weinig lucratief om met de gegevens van één persoon te frauderen. Het wordt pas interessant om in één keer met de gegevens van een grotere groep personen toe te slaan.

Dat het aantal fraudezaken in de tijd minder is geworden, is een gevolg van het feit dat uitvoeringsorganisaties hun beveiligingsniveaus hebben verhoogd en bij het vermoeden van fraude snel actie ondernemen. Het hogere veiligheidsniveau heeft ervoor gezorgd dat het voor gelegenheidsfraudeurs lastig is om bij deze organisaties te frauderen en zijn het vooral criminele organisaties die een poging doen om te frauderen.

3.2 Gemeenten

De meeste gemeenten krijgen geen meldingen

Van de negen geïnterviewde gemeenten geven zeven gemeenten aan dat zij niet of nauwelijks met slachtoffers van identiteitsfraude te maken hebben gekregen. Fraude door bijvoorbeeld bijstandsuitkeringen aan te vragen op andermans naam is nagenoeg niet mogelijk, omdat aanvragers in persoon moeten verschijnen en hun identiteit ter plaatse wordt vastgesteld.

De grotere steden, met name Amsterdam en Den Haag, melden dat identiteitsfraude wel degelijk voorkomt. Het Team Identiteitsfraude (TIF, zie kader) Amsterdam meldt dat ze per jaar tussen de 10 en 15 gevallen van documentfraude signaleren en enkele tientallen gevallen van mensensmokkel. Daarnaast zijn er (enkelvoudige) fraudezaken aan het loket en wijzigingen in rekeningnummer bij het uitkeren van toelagen[19].

Team Identiteitsfraude (gemeente Amsterdam)

Team Identiteitsfraude (TIF) is een samenwerkingsverband tussen de gemeente Amsterdam en de Nationale Politie, eenheid Amsterdam. Het TIF nodigt slachtoffers uit op het gemeentehuis voor een gesprek en vaak sluit ook een politieagent aan bij het gesprek. Ze denken mee met het slachtoffer en kijken of hij of zij alle schade goed in kaart heeft. Het TIF zet alles voor de burger op een rijtje en maakt een onderzoeksrapport. Op die manier heeft de burger een kant en klaar verhaal om mee naar het CMI te gaan. TIF krijgt geen feedback van het CMI, maar er zijn na doorverwijzing nog geen slachtoffers bij hen teruggekomen.

Deze intensieve aanpak is overigens een beleidskeuze van de gemeente Amsterdam; het is geen (wettelijke) taak van gemeenten om slachtoffers van identiteitsfraude te helpen.

Bron: Interview met gemeente Amsterdam/TIF

3.3 Private organisaties

Het aantal meldingen van slachtoffers in de private sector verschilt per branche. Hieronder beschrijven we op grond van het onderzoek voor een aantal branches de uitkomsten.

Thuiswinkelbranche: jaarlijks honderden slachtoffers

Online webwinkels hebben veel te maken met zogenaamde betaalfraude. Bij betaalfraude wordt in dit geval virtueel misbruik gemaakt van betaalkaarten of de gegevens die erop staan. De geïnterviewde webwinkels hebben jaarlijks met enkele honderden meldingen van slachtoffers van identiteitsfraude te maken, vooral met slachtoffers waarvan de bankrekening is gehackt (door bijvoorbeeld phishing). Het hacken van (vaste) klantaccounts komt minder vaak voor en meestal in bepaalde periodes, wat er volgens de webwinkels op duidt dat er een criminele organisatie actief is.

[19] Een van de gemeenten merkt op dat identiteitsfraude niet voorkomt, maar documentfraude wel. Deze gemeente heeft als gevolg hiervan geen aanpak rondom identiteitsfraude, maar wel voor documentfraude.

Telecomsector: Geen eenduidig beeld

Uit de gesprekken met de drie telecombedrijven is niet duidelijk geworden hoeveel slachtoffers zich jaarlijks melden. Een telecombedrijf gaf aan vrijwel nooit met slachtoffers van identiteitsfraude te maken hebben; een ander bedrijf had dit juist wel regelmatig. Ook meldt een telecombedrijf dat identiteitsfraude in het verleden vaak voorkwam, maar nu bijna niet meer. Dit heeft alles te maken met aanpassingen in de leveringsprocedure (thuisbezorging door bezorgers die getraind zijn in identiteitscontroles; daarnaast moeten klanten en een klein bedrag overmaken, waarmee de identificatie wordt gekoppeld aan het bankrekeningnummer van de klant).

Zorgverzekeraars: weinig slachtoffers

Twee van de vier zorgverzekeraars die aan het onderzoek hebben meegedaan, verstrekken cijfers over het aantal slachtoffers van identiteitsfraude onder hun klanten. In beide gevallen gaat het om circa 5 gevallen per jaar. Eén van de andere zorgverzekeraars noemt geen aantallen, maar merkt wel op dat het aantal slachtoffers stijgt. Als zorgverzekeraars signalen ontvangen, dan nemen zij deze in onderzoek.

Bankensector: scherpe daling

Tot voor kort heeft de bankensector veel te maken gehad met schade door fraude in het betalingsverkeer, vooral door skimming en phishing. Cijfers over aantallen meldingen zijn niet beschikbaar (zie paragraaf 2.2 voor aantallen incidenten. Uit de cijfers over de schadeomvang blijkt dat de totale schade is gedaald van € 33,3 miljoen in 2013 naar € 17,3 miljoen in 2014[20]. In 2012 bedroeg de schade nog € 81,8 miljoen (zie verder paragraaf 2.3). De daling is volgens de NVB het gevolg van de gezamenlijke inspanning van banken, politie, Openbaar Ministerie (OM) en consumenten.

3.4 Overige organisaties

Logius

Logius geeft DigiD's uit aan burgers en verzorgt het gebruik van DigiD als authenticatiemiddel bij e-dienstverlening van (semi-)overheden. Na enkele publiekelijk bekende voorvallen van grootschalige diefstal van DigiD's, heeft Logius detectiesystemen ingericht om grootschalig misbruik van andermans DigiD op te sporen en te voorkomen.

Zo'n 700 tot 800 keer per jaar melden burgers zich bij de klantenservice (service helpdesk) van Logius, vaak na doorverwijzing van een afnemer, die aangeeft dat hun DigiD is ontfutseld en/of gebruikt door een derde. Deze personen krijgen van de medewerkers van het team Fraudebestrijding van Logius advies (wijziging wachtwoord, aangifte doen) en worden in een deel van de gevallen naar het CMI doorverwezen.

De politie heeft geen cijfers over identiteitsfraude

Om voor compensatie in aanmerking te komen, is het doen van een aangifte bij de politie van belang (zie ook paragraaf 6.1). Doordat identiteitsfraude vaak deel uitmaakt van een ander delict, kan deze vorm van fraude onder verschillende artikelen uit het Wetboek van Strafrecht vallen. Mede als gevolg hiervan heeft de politie geen cijfers

[20] Bron: Jaarverslag NVB 2014, www.nvb.nl

over het aantal zaken van identiteitsfraude. Volgens het Nationaal Dreigingsbeeld is in 80% van de fraudegevallen sprake van enige mate van misbruik van identiteitsdocumenten en/of -gegevens.

Overigens merken zowel publieke, private als hulpverlenende organisaties op dat slachtoffers niet altijd aangifte doen van identiteitsfraude. In de update van het onderzoek '*Omvang van identiteitsfraude en de maatschappelijke schade in Nederland*' (PWC, 2013) schrijft PWC dat van de respondenten die slachtoffer zijn van identiteitsfraude, 36% aangifte heeft gedaan bij de politie. In het onderzoek van Paulissen en Van Wilsem gaat slechts 10% van de slachtoffers naar de politie. Beide percentages zijn mogelijkerwijs niet representatief, omdat ze zijn gebaseerd op een relatief klein aantal slachtoffers. Opvallend is wel dat het in beide gevallen om een klein aandeel gaat dat aangifte doet. Volgens Van Wilsem stappen alleen diegenen die veel geld kwijt zijn, naar de politie. Ook komt het voor dat een slachtoffer bekend is met de dader en dat hij/zij om die reden geen aangifte durft te doen.

LMIO registreert alleen grootschalige zaken

Het Landelijk Meldpunt Internetoplichting (LMIO) is een gecentraliseerde expertafdeling binnen de politie die zich met name bezighoudt met aankoop- en verkoopfraude (oplichting via valse webwinkels, online marktplaatsen, et cetera). Het LMIO krijgt dagelijks meldingen van identiteitsfraude, maar bij slechts een beperkt gedeelte gaat het om identiteitsfraude. Het valt het LMIO op dat het aantal fraudezaken met online banken, waarbij een rekening kan worden geopend op basis van afgeleide identificatie, toeneemt.
Het LMIO ziet regelmatig dat een kopie van een identiteitsbewijs meerdere keren wordt gebruikt om te frauderen. Bijvoorbeeld op Marktplaats, waar de verkoper als teken van vertrouwen een kopie van zijn (gestolen) identiteitsbewijs stuurt en er ook één van de klant vraagt. Op deze wijze verzamelt de dader ook direct nieuwe kopieën waarmee hij/zij fraude kan plegen.
Het LMIO kan (nog) geen exacte aantallen genereren, maar ontwikkelt een database waarin identiteitsfraude afzonderlijk wordt genoteerd. De organisatie verwacht in 2016 cijfers te kunnen genereren over het aantal meldingen van identiteitsfraude in 2015.

Het Openbaar Ministerie

Het is mogelijk om bij het Openbaar Ministerie (OM) aangifte te doen van identiteitsfraude. In de meeste gevallen maken slachtoffers hier geen gebruik van, omdat zij naar de politie gaan om aangifte te doen. Het OM heeft dan ook vooral contact met slachtoffers wanneer zij een zaak beginnen of het OM daartoe verzoeken.
Het OM ziet identiteitsfraude als een groot probleem, omdat het modus operandi is voor een ander delict. In veel fraudegevallen is er in enige mate sprake van misbruik van identificerende persoonsgegevens; het aantal 'schrijnende gevallen' is echter op één hand te tellen.

CBP krijgt vrijwel geen meldingen

Het College bescherming persoonsgegevens (CBP) is toezichthouder waar het gaat om de naleving van de Wet bescherming persoonsgegevens (Wbp) door overheden en bedrijven. De organisatie heeft wel eens contact (telefonisch of via een tipformulier op de website) met bezorgde burgers die bang zijn dat er met het afgegeven kopie van identiteitsdocumenten risico is op identiteitsfraude. Het CBP verwijst in dergelijke gevallen soms door naar het CMI en/of attendeert mensen op veiliginternetten.nl.

Het CBP richt zich, binnen de kaders van de Wbp, in het licht van (risico op) identiteitsfraude, op:

- voorlichting geven aan burgers en (branche-)organisaties via richtsnoeren en Q&A's op de website over onder meer dataminimalisatie en over 'privacy by design', en
- compliance met de Wbp bewerkstelligen. Het CBP heeft de bevoegdheid om ambtshalve of op verzoek van een belanghebbende onderzoek te doen naar de naleving van de Wbp. Het CBP kan zo'n onderzoek bijvoorbeeld starten vanwege actuele gebeurtenissen of tips die het CBP ontvangt over mogelijke overtredingen van de wet.

3.5 Meldpunten en hulpverlenende organisaties

Naast voorgaande instanties melden slachtoffers van identiteitsfraude zich ook bij diverse meldpunten en hulpverlenende organisaties[21]. Hieronder staat per organisatie het aantal meldingen van (identiteits-) fraude dat zij ontvangen:

- Het *Centraal Meldpunt Identiteitsfraude en -fouten* (*CMI)* heeft in 2014 884 meldingen van identiteitsfraude ontvangen van particulieren. In 2012 bedroeg het aantal meldingen nog 291, in 2013 verdubbelde dat aantal naar 612. Meer dan 90% van de meldingen betrof fraude (de overige 10% betrof fouten). De meeste fraude vond plaats met een kopie van een ID-bewijs in de e-commerce en bancaire sector.
- De *Fraudehelpdesk* heeft over heel 2014 790 meldingen van identiteitsfraude binnen gekregen. In juni 2015 stond de teller op bijna 700 meldingen. In beide gevallen gaat het voornamelijk om identiteitsfraude waarbij oplichters de identiteit van een bedrijf aannemen. In 2014 zijn 74 meldingen doorgestuurd naar het CMI; in deze gevallen gaat het om particuliere slachtoffers. Verder kwamen bij de Fraudehelpdesk in 2014 13 meldingen binnen van gebruik van valse ID-documenten. Tot 1 december 2014 kreeg de Fraudehelpdesk 41.466 phishing-mails doorgestuurd (mails waarvan de URL op de zwarte lijst staat)[22].
- *Slachtofferhulp Nederland* helpt zo'n 150.000 slachtoffers per jaar. Het aantal slachtoffers van identiteitsfraude zijn naar schatting hooguit enkele tientallen slachtoffers per jaar[23].
- De *Nationale Ombudsman* schat dat het aantal slachtoffers van identiteitsfraude dat zich bij hen meldt, enkele gevallen per jaar zijn. De aantallen zijn lastig vast te stellen, omdat identiteitsfraude vaak onderdeel uitmaakt van een ander delict en zaken dus niet altijd gemeld worden als identiteitsfraude.

3.6 Conclusie

Zowel publieke als private organisaties registreren incidenten van identiteitsfraude niet (als afzonderlijke categorie) en/of zijn niet bereid deze cijfers te delen. Het aantal (meldingen van) incidenten van identiteitsfraude is daardoor veelal niet bekend.

Publieke en private organisaties zien dat fraude met (kopieën van) identiteitsdocumenten en DigiD's weinig voorkomt, meldingen van deze fraudevorm bij het CMI nemen wel toe. In de private sector vormt identiteitsfraude via internet (phishing en pharming) een probleem dat veelvuldig voorkomt; positief is dat in de bancaire sector skimming sterk is afgenomen.

De aantallen meldingen van burgers die zelf met een vermoeden van identiteitsfraude aankloppen, zijn klein. Verreweg de meeste gevallen

[21] Zie hoofdstuk 6 voor een nadere beschrijving van deze organisaties.

[22] Identiteit in cijfers, Panteia, 2014.

[23] Slachtofferhulp Nederland heeft geen aparte registratie van gevallen van identiteitsfraude, deze casussen worden geregistreerd onder het thema fraude.

komen aan het licht door een onderzoek gestart door de desbetreffende organisatie.

4 Behandeling door publieke organisaties

Dit hoofdstuk beschrijft de afhandeling van identiteitsfraude door overheidsorganisaties. De eerste paragraaf behandelt de afwikkeling van fraudezaken door uitvoeringsorganisaties (Belastingdienst, DUO, KvK, RDW, SVB en UWV) en de tweede paragraaf gaat in op gemeenten.

4.1 Uitvoeringsorganisaties

4.1.1 Focus op preventie

Identiteitsfraude op agenda van ketenoverleg

Binnen het openbaar bestuur zijn in de afgelopen paar jaar enkele ketenoverleggen gestart, waarbinnen identiteitsfraude een plek heeft gekregen. Zo is er het ketenoverleg CMI (RDW, BD, EVIM, Logius, OM, IND, Matchingsautoriteit, ECID en de politie, onder regie van het CMI), het overleg binnen de voertuigketen (waarin de RDW, CJIB, OM, en de politie participeren), en de Werkgroep Tegengaan Identiteitsfraude binnen de politieregio Oost-Nederland (politie, OM, gemeenten, RDW en andere). In deze overleggen worden (nadere) afspraken over ketensamenwerking gemaakt, overleg gevoerd over complexe casussen en ontwikkelingen rondom identiteitsfraude (bijvoorbeeld nieuwe vormen) besproken.

Uitvoeringsorganisaties nemen preventieve maatregelen

De geïnterviewde uitvoeringsorganisaties nemen allemaal maatregelen om misbruik van identiteiten te voorkomen. Verificatie van ingediende aanvragen of wijzigingen bij de betrokkene zelf is daarbij een belangrijk principe. Dat gebeurt onder andere met de tweestaps authenticatie van DigiD (code en sms-authenticatie) of per post, e-mail of via de berichtenbox van mijnoverheid.nl. Ook zijn softwaresystemen aangepast (zodat mogelijke fraude snel wordt gesignaleerd), zijn gespecialiseerde fraudeteams actief, wisselen partijen onderling signalen van mogelijke fraude uit en worden bankrekeningnummers gecontroleerd.

Fraudeteam Logius: hoger beveiligingsniveau DigiD

Na incidenten in 2013 heeft Logius maatregelen getroffen om nieuwe fraudegevallen te voorkomen. Er is een fraudeafdeling opgericht, die in de eigen systemen signalen van identiteitsfraude opspoort en aanpakt[24].

Burgers ook zelf verantwoordelijk

De uitvoeringsorganisaties zorgen intern voor een hoog beveiligingsniveau van de eigen systemen en werken samen met Logius om de veiligheid van het gebruik van DigiD te garanderen. Dit neemt niet weg dat klanten ook zelf verantwoordelijk zijn voor een veilig gebruik van identificatiedocumenten en -gegevens.

Overheidscampagnes stimuleren dan ook tot terughoudendheid bij het laten kopiëren van identiteitsbewijzen, door gebruik van een 'ID-cover' die pasfoto, BSN, documentnummer en de enkel door machines leesbare zone afdekt, en door op de kopie 'kopie', afgiftedatum en -doel te zetten. Op www.digid.nl/veiligheid staan verder veiligheidstips van DigiD, waaronder het devies 'Houd je DigiD privé' en het gebruik van de DigiD-machtiging in plaats van het verstrekken van de eigen DigiD aan derden (bijvoorbeeld wanneer een familielid of belastingadviseur helpt bij het aanvragen van een toeslag). UWV wijst er bijvoorbeeld op dat het van belang is dat

[24] Individuele fraudegevallen worden via de helpdesk van Logius geholpen.

klanten gebruikmaken van de aangeboden extra beveiliging, zoals de sms-authenticatie.

Slachtoffers van exen fraude

Veel meldingen die binnenkomen bij de hulp- en dienstverlenende organisaties betreffen misbruik van identiteit door (voornamelijk) ex-partners en directe familieleden. Bij ex-partners is het doel van de ex-partner in de meeste gevallen om de ander in de problemen te brengen (het leven zuur te maken), financieel gewin is meestal ondergeschikt. Bij directe familie gaat het wel vaak om financieel gewin. Geïnterviewde overheidsorganisaties geven in praktisch alle gevallen aan dat zij slachtoffers van fraude in de relationele sfeer niet kunnen helpen bij het terugdraaien van transacties of besluiten. De kern van het probleem is dat er bij een relationeel geschil geen rol is weggelegd voor de overheid: men kan zich niet in deze privaatrechtelijke discussie mengen. Daarnaast zijn de identificerende gegevens zelf vaak door het slachtoffer ter beschikking gesteld (of in ieder geval toegankelijk gemaakt) aan de dader. Het CMI krijgt wel veel meldingen van deze groep en probeert hen te begeleiden, met name door adviezen te geven (aangifte, wijzigen van wachtwoorden).

Het is relevant om in dit kader te melden dat driekwart van de Nederlanders de meeste verantwoordelijkheid voor het *voorkomen* van identiteitsfraude bij de burger zelf legt[25]. Dat ligt anders bij het *oplossen* van identiteitsfraude: hier legt 68 procent de meeste verantwoordelijkheid bij de overheid.
PWC stelt in dit onderzoek ook dat Nederlanders al diverse maatregelen nemen om identiteitsfraude te voorkomen: 86 procent zegt geen persoonlijke gegevens aan onbekenden te geven, eveneens 86 procent deelt geen pincodes of wachtwoorden met derden en 85 procent zegt slechts beperkt persoonsgegevens via telefoon of internet te delen. Ook geeft 83 procent aan goed op bankpasjes en creditcards te letten en 78 procent zegt documenten als rijbewijs en paspoort goed te bewaren. Minder Nederlanders nemen maatregelen als het beveiligen van de brievenbus (17 procent) en het regelmatig wijzigen van wachtwoorden en pincodes (43 procent). Slechts 3 procent geeft aan geen van deze en andere maatregelen te treffen.

[25] PWC, 2013-update onderzoek 'Omvang van identiteitsfraude & maatschappelijke schade in Nederland (Amsterdam, mei 2013).

4.1.2 Begeleiding van slachtoffers van identiteitsfraude

Specifieke medewerker of afdeling voor identiteitsfraude

Indien burgers die mogelijk te maken hebben met identiteitsfraude zich melden bij de telefonische frontoffice van de uitvoeringsorganisaties, worden deze volgens de organisaties zelf in principe doorgeleid naar centrale aanspreekpunten, ofwel aangewezen medewerkers of afdelingen (meestal een afdeling Handhaving). Dit is volgens de uitvoeringsorganisaties een ontwikkeling van grofweg de laatste twee jaar, waarin identiteitsfraude beter op het netvlies staat.
Het CMI meldt dat er in de backoffice van de overheidsorganisaties inmiddels aanspreekpunten zijn, maar dat het voor de slachtoffers vaak nog een behoorlijke klus kan zijn om daar met de melding terecht te komen. Het CMI bemiddelt dan en zorgt dat de juiste afdeling betrokken wordt. Logius meldt daarentegen dat ze recentelijk nauwelijks van burgers vernomen hebben dat men bij de overheidsorganisaties nul op rekest krijgt.

Helpdesks voor vragen rondom DigiD's

In het geval van fraude met DigiD's komen slachtoffers in eerste instantie bij de DigiD helpdesk terecht. Daar wordt het gros van alle vragen afgehandeld. De overige vragen gaan door naar het Logius servicecentrum. In geval van fraude worden melders direct doorverwezen naar Logius.

Bron: Interview Logius

Na melding slachtoffer of signaal volgt een intern onderzoek

De interne aanspreekpunten binnen uitvoeringsorganisaties voeren na een melding of een signaal (uit de eigen organisatie of via Logius) een onderzoek uit binnen de eigen systemen. Zij onderzoeken waar en wanneer de fraude heeft plaatsgevonden en welke klanten eventueel ook zijn geschaad.

Wanneer DigiD het identificatiemiddel is geweest, gebeurt het onderzoek in samenspraak met Logius. Logius blokkeert de DigiD's en stuurt de betrokkenen een brief waarin het voorval wordt gemeld. Ook worden de afnemers geïnformeerd waarvan Logius kan waarnemen dat het gestolen DigiD er is gebruikt.

De Belastingdienst merkt aangaande het interne onderzoek op dat dit onderzoek sneller in gang gezet kan worden, indien het CMI (wanneer het betrokken is bij een casus) een explicietere probleembeschrijving kan leveren. Dit helpt om de fraude binnen de eigen organisatie te traceren.

Samenwerking met andere organisaties

Om een melding of signaal van identiteitsfraude goed in kaart te kunnen brengen en zo mogelijk op te lossen, werken de geïnterviewde uitvoeringsorganisaties vrijwel allemaal samen met derden. De belangrijkste partijen zijn:

- Logius, wanneer er sprake is van misbruik van DigiD's;
- de politie, voor het uitvoeren van nader onderzoek;
- het CMI, voor de begeleiding van het slachtoffer.

Waar relevant worden ook andere ketenpartners bij een casus betrokken.

Contact met slachtoffers

De interne aanspreekpunten onderhouden gedurende het gehele proces contact met slachtoffers wanneer zij een melding hebben gedaan. Wanneer er signalen zijn op grond van intern onderzoek of een melding van Logius, dan wordt bij bevestiging van het vermoeden van fraude de burger in principe direct telefonisch geïnformeerd of zelfs soms persoonlijk bezocht om het voorval te bespreken. De SVB geeft nog aan dat bij zaken met grote aantallen (potentiële) slachtoffers een calamiteitenteam ingericht wordt dat de burgers bezoekt.

De (mogelijke) slachtoffers worden op de hoogte gehouden van de voortgang en resultaten van het onderzoek en worden geadviseerd om aangifte te doen.

Maatregelen om verdere financiële schade slachtoffers te voorkomen

Naast dit persoonlijke contact treffen uitvoeringsorganisaties bij een vermoeden van identiteitsfraude maatregelen, om verdere financiële schade voor slachtoffers te voorkomen. De Belastingdienst en de RDW zetten bijvoorbeeld bij een dergelijk vermoeden eventuele inningen stop; de SVB, DUO en UWV verstrekken aan slachtoffers

eventuele (waarschijnlijk) onterecht niet ontvangen uitkeringen en/of toeslagen.

Herstel van registraties

Wanneer er sprake blijkt van identiteitsfraude dienen de uitvoeringsorganisaties de gegevens in hun registratie te herstellen. Het gaat dan om bijvoorbeeld onjuiste bankrekeningnummers en een verkeerde tenaamstelling van een voertuig. Voor persoonsgegevens, zoals het adres, zijn uitvoeringsorganisaties afhankelijk van de BRP, die door gemeenten wordt beheerd.

De KvK voert, als een identiteitsbewijs is opgenomen in het VIS (zie paragraaf 3.1), de gewenste mutatie van bedrijfsgegevens niet door. In deze gevallen krijgt de KMAR automatisch een melding. De KvK doet daarnaast bij de politie aangifte van misbruik van het handelsregister als een mutatie wel is doorgevoerd (en dus niet door het VIS als vermist is herkend.

RDW: herstel van schade

De RDW heeft een afspraak met de Ombudsman dat meldingen van identiteitsfraude binnen zes weken worden uitgezocht. In de praktijk is dit een kleine drie maanden. Uit zorgvuldigheid worden alle dossiers binnen de RDW door twee personen behandeld. Wanneer er daadwerkelijk sprake is van identiteitsfraude lost de RDW op de volgende manieren de ontstane gevolgen op:

- *Boetes*: Eventuele onterecht opgelegde boetes laat de RDW automatisch vervallen. Dit proces verloopt intern lastiger wanneer de boetes al door het slachtoffer zijn voldaan.
- *Tenaamstelling*: Om een foutieve tenaamstelling te beëindigen is een aangifte van identiteitsfraude noodzakelijk. Het beëindigen van de tenaamstelling kan vanaf de datum van het proces verbaal en in principe niet met terugwerkende kracht. Sinds 2014 kan de RWD, unit APR, bij gemaakte fouten ook met terugwerkende kracht de tenaamstelling herzien. Op grond van de beëindiging van de tenaamstelling kunnen genomen besluiten, zoals opgelegde boetes, worden herzien. Hiervoor vindt bespreking plaats in het voertuigketenoverleg. De RDW merkt op dat het bij veel slachtoffers niet lukt om de tenaamstelling van het voertuig te wijzigen.

Bron: interview RDW

4.1.3 Compensatie van slachtoffers

Weinig inzicht in de financiële schadelast voor slachtoffers

Zoals beschreven in paragraaf 2.3 bestaat de directe financiële schade in de publieke sfeer voornamelijk uit zaken als boetes, terugvorderingen, gemiste uitkeringen en toelagen. De omvang kan per identiteitsfraudezaak sterk verschillen en doordat de fraudegevallen niet afzonderlijk worden geregistreerd, kan het gemiddelde fraudebedrag niet worden berekend.
Bij DUO, SVB en UWV gaat het vaak om één (eventueel enkele) maand(en) uitkering en/of toeslagen. In deze gevallen merken de slachtoffers snel dat zij geen studiefinanciering, uitkering of toeslag hebben gekregen en trekken zij bij de desbetreffende uitvoeringsorganisatie aan de bel. Bij de Belastingdienst kan de hoogte van de financiële schade per geval sterk verschillen. De Belastingdienst kent verschillende soorten toeslagen, waarbij de hoogte afhankelijk is van inkomen, gezinssamenstelling en dergelijke.
Bij de RDW bestaat de financiële schade uit boetes die voortvloeien uit voertuiggebonden verplichtingen (dat wil zeggen boetes voor het

niet verzekeren en het ontbreken van een Algemene Periodieke Keuring).

Snelle compensatie van directe financiële schade

Compensatie van directe financiële schade vindt vrij snel plaats. Geïnterviewde uitvoeringsorganisaties geven aan dat, mits voldoende aannemelijk is dat de identiteitsfraude heeft plaatsgevonden en het slachtoffer daar geen directe schuld aan heeft, compensatie in beginsel altijd plaatsvindt. Het kunnen tonen van een proces-verbaal is daarbij een noodzakelijke voorwaarde.

Compensatie van indirecte (financiële) schade vindt niet plaats

Van compensatie van indirecte schade is zelden sprake.[26] Leges voor eventuele nieuwe identiteitsdocumenten worden bijvoorbeeld niet vergoed. Burgers doen hier over het algemeen ook geen beroep op, noch direct bij de organisatie, noch via een civiele procedure, wat ook bewezen wordt door de beperkte jurisprudentie (zie hoofdstuk 7). Gevallen waarbij een vergoeding heeft plaatsgevonden van indirecte schade (in de vorm van een tegemoetkoming) zijn er wel, bijvoorbeeld in de zaak Kowsoleea[27]. Het gaat hier echter om uitzonderingen.

4.2 Gemeenten

Om een beeld te krijgen van de begeleiding van identiteitsfraude bij gemeenten zijn vertegenwoordigers van 9 gemeenten geïnterviewd. Deze gesprekken leiden niet tot een representatief beeld van het handelen van gemeenten op dit vlak, maar geven hier wel een indicatie van.

Gemeenten merken op dat zij niet of nauwelijks te maken krijgen met identiteitsfraude (zie paragraaf 3.2). De grote gemeenten, zoals Amsterdam en Den Haag, hebben begeleiding geregeld. Enkele andere grote gemeenten geven aan zich op hulpverlening en het inrichten van procedures voor slachtoffers van identiteitsfraude te bezinnen. Een van de geïnterviewde gemeenten merkt expliciet op dat identiteitsfraude zo weinig voorkomt, dat er per casus wordt gekeken hoe de gemeente het slachtoffer kan helpen.

Modelprotocol, vooral gericht op inschrijving

Er bestaat wel een modelprotocol dat is opgesteld door de Nederlandse Vereniging van Burgerzaken, maar dat is vooral gericht op het voorkomen van identiteitsfraude aan de voorkant bij de inschrijving van de BRP. Het protocol adviseert slachtoffers van identiteitsfraude door te verwijzen naar het CMI.

Actief om verkeerde inschrijvingen te voorkomen

Gemeenten zijn wel meer bezig met het voorkomen van fraude met identiteiten bij de inschrijving van personen in de basisregistratie personen en tussen gemeenten wordt op dit gebied ook de samenwerking gezocht (onder andere Enschede, Groningen, veiligheidsregio Oost-Brabant). Deze inzet op de voorkant van het BRP is van belang, volgens TIF, om te voorkomen dat fraudeurs hun slag slaan in gemeenten met een lager beveiligingsniveau.

[26] Als er geprocedeerd wordt en het slachtoffer wint, dan krijgt hij wel de proceskosten (forfaitair) vergoed.

[27] In deze zaak geeft Imro Cairo zich uit voor de zakenman Ron Kowsoleea. Vanaf dat moment worden de delicten van Cairo gekoppeld aan de naam Kowsoleea. Het duurt 19 jaar voordat de zaak is opgelost en de identiteit van de heer Kowsoleea is hersteld.

Het corrigeren van de BRP kan een belemmering vormen[28]

Gegevens in de BRP zijn op grond van de wet als authentiek verklaard en overheidsorganisaties zijn verplicht deze 'voor waar' aan te nemen, tenzij er gerede twijfel bestaat over de juistheid van het gegeven. De inschrijving op zichzelf en de waarde van gegevens hebben niet alleen een identificerende werking, maar kwalificeren een persoon om al dan niet voor een overheidsvoorziening in aanmerking te komen. Brieven gaan naar het gewijzigde adres, belastingheffing wijzigt, uitkeringen worden aangepast, et cetera. Met het oog op deze gevolgen zijn de wijzigingen in de BRP met extra waarborgen omkleed.

Gemeenten zijn niet zonder meer bevoegd om adreswijzigingen (vanwege de terugwerkende kracht) te corrigeren en vragen daarvoor de nodige bewijsstukken. Bovendien is de correctieprocedure complexer dan de mutatieprocedure en kennen niet alle medewerkers van de gemeenten het verschil. Bij het terugdraaien van een adreswijziging met een mutatieprocedure blijft de tijdelijke adreswijziging in de BRP geregistreerd met alle (rechts)gevolgen van dien. Bij een correctie wordt de mutatie geacht niet te hebben plaatsgevonden.

Dergelijke belemmeringen kunnen slachtoffers ervaren wanneer zij bij een gemeente langs gaan om hun gegevens te corrigeren en daartoe om een van de voornoemde redenen niet in de gelegenheid worden gesteld. Het CMI kan in dat soort gevallen met de bewuste gemeente contact opnemen en bemiddelen, maar de wijziging blijft de verantwoordelijkheid van de gemeente.

[28] Deze passage is opgenomen om aan te geven dat het herstel van gegevens in bepaalde systemen, zoals de BRP, erg lastig is, en zonder hulp van een bemiddelde instantie zoals het CMI, bijna onmogelijk.

4.3 Conclusies

Identiteitsfraude staat op de agenda bij de uitvoeringsorganisaties. Er vindt gezamenlijk overleg plaats en de organisaties nemen preventieve maatregelen, om het risico op identiteitsfraude zoveel mogelijk te voorkomen. De organisaties hebben een specifieke medewerker of afdeling gericht op (identiteits-)fraude, voeren onderzoek uit naar aanleiding van meldingen en/of signalen (zowel intern als van Logius) en proberen de fraude te beëindigen. In dit proces hebben zij aandacht voor het slachtoffer, dat door de fraude niet alleen financieel maar ook emotioneel geraakt is. Uitvoeringsorganisaties compenseren directe financiële schade als uit intern onderzoek het vermoeden van fraude terecht lijkt en in veel gevallen nadat het slachtoffer aangifte heeft gedaan.
Gemeenten hebben geen wettelijke taak waar het gaat om identiteitsfraude. Doordat de meeste geïnterviewde gemeenten geen meldingen hebben van identiteitsfraude, hebben zij ook geen (geprotocolleerde) aanpak. Enkele grote gemeenten hebben daarentegen wel een aanpak gericht op het voorkomen en verhelpen van identiteitsfraude. Het zijn ook deze gemeenten die wel melding maken van identiteitsfraudezaken in hun gemeente.

5 Behandeling door private organisaties

Dit hoofdstuk schetst een beeld van de afhandeling van identiteitsfraude door private organisaties. De interviews zijn uitgevoerd in de thuiswinkelbranche, de banken- en telecomsector, en bij (semi-private) zorgverzekeraars, de Beroepsorganisatie van Notarissen (KNB) en PostNL. Het aantal geïnterviewde partijen is niet voldoende om uitspraken te doen die voor de verschillende sectoren representatief zijn; het beeld moet dus gezien worden als een indicatie.

5.1 Focus op preventie

Op grond van de interviews bestaat het beeld dat de meeste private organisaties, en zeker de bancaire sector, zich proactief opstellen en zich inzetten om nieuwe fraudegevallen te voorkomen.

Tal van preventieve maatregelen

Geïnterviewde bedrijven nemen tal van maatregelen om fraude (waaronder ook identiteitsfraude) tegen te gaan. Standaardmaatregelen zijn onder meer:

- Controle van de geldigheid van identiteitsdocumenten in het Verificatieregister (paspoorten en ID-kaarten) en het rijbewijzenregister; vaak via intermediaire organisaties als BKR, Experian en ID-checker.
- Controle van creditcardgegevens bij de desbetreffende maatschappij.
- Controle aan de hand van een interne of met andere bedrijven gedeelde 'black list'.
- Controle identiteitsbewijs bij aflevering product of voor een operatie in het ziekenhuis (aan de hand van een checklist met legitimatievoorschriften).
- Gebruik van kopie identiteitsbewijs alleen in combinatie met ideal-transactie.
- Gebruik van geoblocking, waardoor vanuit het buitenland (buiten Europa) geen aankopen gedaan kunnen worden.
- Nieuw relatie-/klantnummer om toekomstig misbruik tegen te gaan.
- Een protocol voor de klantenservice om te voorkomen dat (medische) informatie wordt vrijgegeven aan 'kwaadwillende' derden, zoals een ex-partner of een schuldeiser.

Overigens nemen niet alle private organisaties dergelijke maatregelen. In de thuiswinkelsector maakt identiteitsvaststelling geen deel uit van het aankoopproces, maar wordt gecontroleerd aan de hand van het betaalmiddel. Bij (kleine) online banken is er sprake van afgeleide identificatie: de klant komt niet persoonlijk langs maar identificeert zichzelf met een kopie van een identiteitsbewijs.
De aard van de dienstverlening van dergelijke private partijen brengt met zich mee dat deze sector zich genoodzaakt ziet identiteitsfraude als een bedrijfsrisico te zien en dit in hun verdienmodel te incalculeren. De dienstverlening van deze bedrijven is door een lager beveiligingsniveau (ook voor fraudeurs) makkelijker toegankelijk en ze zijn tegelijkertijd bereid de geleden schade te compenseren.

Uitwisseling van kennis en ervaringen tussen bedrijven

Om fraudegevallen op te lossen en te voorkomen, hebben bedrijven de behoefte om onderling informatie uit te wisselen, bijvoorbeeld over fraudevormen. Dit soort informatie wordt één-op-één gedeeld, maar komt ook in georganiseerd verband voor, zoals bij de werkgroep fraude en veiligheid van Thuiswinkel.org.
De snelheid waarmee fraudeurs hun strategie kunnen aanpassen, versterkt de behoefte van bedrijven om onderling kennis uit te

wisselen en ervoor te zorgen fraudeurs een stap voor te blijven. Ook het gegeven dat fraudeurs meerdere webshops of telecombedrijven tegelijkertijd oplichten, benadrukt het belang van onderling informatie delen. Het is om die reden dat er binnen het bedrijfsleven behoefte bestaat aan verdergaande stappen, zoals het delen van 'valse identiteiten' en/of persoonsgegevens van (vermoedelijke) fraudeurs via een database en/of blacklist. Dit zou hen helpen om fraude te voorkomen. Eén van de respondenten ziet het Britse Cifas in dit kader als goed voorbeeld (zie kader). Een dergelijke uitwisseling is als gevolg van restricties binnen de Wet bescherming persoonsgegevens niet mogelijk.

CIFAS, database voor bedrijven

Cifas, een Britse not-for-profit organisatie, beheert een 'nationale fraude database'. Jaarlijks voegen bedrijven uit verschillende sectoren meer dan 200.000 bevestigde fraudegevallen toe. Bedrijven die lid zijn van Cifas, kunnen bij transacties extra controles uitvoeren aan de hand van de database en zo checken of iemand betrokken is geweest bij een fraudegeval. Hierdoor is het aantal fraudegevallen in Groot-Brittannië gedaald, aldus Cifas.
Bron: www.cifas.org.uk

Uitwisseling met overheidsinstanties

Naast kennisuitwisseling tussen private partijen onderling, bestaat er ook behoefte aan uitwisseling met overheidsinstanties. Enkele private partijen melden behoefte te hebben aan ketenoverleg onder andere met het CMI. Twee partijen maken melding van een convenant: de ene partij wilde er één afsluiten met de politie, de ander was in gesprek met een hulpofficier van justitie. In beide gevallen is het convenant blijven liggen, ondanks dat er interesse was vanuit andere partijen.

5.2 Begeleiding van slachtoffers van identiteitsfraude

Eerste aanspreekpunt?

De meeste geïnterviewde bedrijven geven aan dat het slachtoffer in principe geholpen wordt en dat het fenomeen goed op de radar staat. Na melding wordt het slachtoffer intern doorverwezen naar de gespecialiseerde medewerker en/of afdeling. Met name banken hebben een aanspreekpunt ingericht. Het CMI heeft de ervaring dat slachtoffers bij sommige bedrijven, vooral in de telecomsector, moeite hebben om hun situatie in behandeling te krijgen als fraudegeval. Klanten wordt verzocht de formele route van bezwaar of klacht te volgen en worden niet doorverbonden met een op identiteitsfraude gespecialiseerde afdeling of medewerker.

Onderzoek naar de fraude

De private organisaties onderzoeken, evenals in de publieke sector, de aannemelijkheid van de fraude en nemen op basis daarvan besluiten over eventuele compensatie. Een partij gaat daarbij verder, aldus de geïnterviewde: omdat de klant de fraude veelal niet kan overzien helpt het bedrijf de klant met het in kaart brengen van hoe de fraude is gestart en waar eventueel nog meer gefraudeerd kan zijn.

Doorverwijzen van slachtoffers

Uit de interviews komt het beeld naar voren dat relatief weinig private organisaties slachtoffers doorverwijzen naar instanties die begeleiding bieden. Vrijwel geen van de geïnterviewde private partijen verwijst door naar het CMI (zie ook paragraaf 6.2.1), enkele bedrijven sturen slachtoffers door naar de Fraudehelpdesk (zie ook paragraaf 6.2.2).

Aangifte doen

Enkele private organisaties stellen als voorwaarde voor compensatie van geleden schade dat slachtoffers aangifte doen bij de politie. Deze aangifte is van belang voor nader onderzoek door de politie. Een van de private partijen merkt daarbij expliciet op dat aangifte ook in het belang van het slachtoffer is, namelijk in het geval dat diens identiteit op meerdere plaatsen wordt misbruikt. De aangifte helpt het slachtoffer volgens de geïnterviewde om de fraude te bewijzen. Hierbij dient opgemerkt te worden dat het formeel zo is dat de bewijslast van de identiteitsfraude bij de verkopende partij ligt en niet bij het slachtoffer. Het CMI moet een slachtoffer daar nogal eens op wijzen, hetgeen er op duidt dat niet iedereen daarvan op de hoogte is.

Medewerking aan politie

Vaker dan dat private organisaties slachtoffers adviseren om aangifte te doen, benadert de politie deze organisaties voor nader onderzoek. Deze bedrijven helpen de politie, zoals zij behoren te doen, door het beschikbaar stellen van data en eventueel videobeelden, bijvoorbeeld van een dader die een online aangekocht product in de winkel komt afhalen. Overigens merken ook enkele partijen op dat de politie vaak (als gevolg van een gebrek aan capaciteit en/of kennis) geen nader onderzoek instelt, dat dit enkel gebeurt wanneer er sprake is van grootschalige fraude. Een andere partij herkent dit beeld niet en merkt op dat onderzoek van de politie afhankelijk is van de aard en ernst van het incident en de mogelijkheden van de politie om onderzoek te doen.

5.3 Compensatie van slachtoffers

Compensatie na onderzoek

Tot het afwikkelen van een fraudezaak behoort ook het compenseren voor geleden schade[29]. Private partijen lijken, net als de publieke organisaties, over het algemeen coulant met slachtoffers van identiteitsfraude. Dit heeft te maken met een klantgerichte bedrijfsvoering en het niet willen schaden van het imago.

Net als publieke organisaties onderzoeken private organisaties - voor zover mogelijk - in hun registraties en dossiers of er bewijzen zijn voor de identiteitsfraude. Indien de melder niet verantwoordelijk is voor de transactie, dan gaan private organisaties over tot compensatie. Dit geldt in de meeste gevallen ook voor situaties waarin het bedrijf niet kan aantonen wat de rol van de melder is geweest.
Tegelijkertijd zijn er volgens het CMI signalen van slachtoffers die aangeven dat private partijen niet zo gemakkelijk meewerken wanneer het gaat om compensatie van geleden schade en/of herstel van registraties. Ook de jurisprudentie laat dit zien (zie hoofdstuk 7).

De bancaire sector als voorbeeld

Een van de aanleidingen voor dit onderzoek betrof de motie-Gesthuizen, waarin gesteld wordt dat de overheid zich zou moeten laten inspireren door de coulanceregelingen van banken. Inderdaad zijn banken coulant als het gaat om compensatie van diefstal via identificerende gegevens (skimming, phishing, trojan horses, et cetera). Wel wordt kritisch gekeken naar de verantwoordelijkheid

[29] De compensatie kan, afhankelijk van de betaalvorm, ook plaatsvinden vanuit de financiële instelling die de betaling organiseert. Als er bijvoorbeeld als gevolg van 'phishing' middels iemands bankrekening producten zijn besteld, dan zal hij of zij de schade moeten verhalen op de bank.

van de klant. Als de bank aan haar zorgplicht heeft voldaan en de gegevens voldoende heeft beschermd (overeenkomstig daarvoor bestaande beveiligingsnormen), wat in de praktijk over het algemeen het geval is, kan de bank weigeren schade te vergoeden als blijkt dat de klant niet aan eigen verplichtingen heeft voldaan, ofwel nalatig is geweest. De NVB heeft hiervoor vijf criteria vastgesteld die leidend zijn (zie kader).

Uniforme veiligheidsregels banken

"Het is voor consumenten wettelijk geregeld dat een bedrag, dat zonder uw toestemming van uw bankrekening is afgeschreven, door de bank wordt vergoed. [...] De bank is echter niet altijd verplicht het bedrag, eventueel verminderd met het eigen risico van maximaal € 150, aan u te vergoeden. Wanneer u zich aan de onderstaande vijf veiligheidsregels houdt, loopt u niet het risico dat de gehele schade voor uw eigen rekening komt.

1. Houd uw beveiligingscodes geheim.
2. Zorg ervoor dat uw bankpas nooit door een ander gebruikt wordt.
3. Zorg voor een goede beveiliging van de apparatuur die u gebruikt voor uw bankzaken.
4. Controleer uw bankrekening.
5. Meld incidenten direct aan de bank en volg aanwijzingen van de bank op.

Bron: Uniforme veiligheidsregels particulieren, NVB

5.4 Conclusie

Binnen de private sector bestaat een wisselend beeld. Het is vooral de bancaire sector die zich actief inzet om identiteitsfraude (en dan vooral skimming en phishing) tegen te gaan. Ook binnen de andere branches worden maatregelen genomen om identiteitsfraude tegen te gaan. Dit geldt niet voor enkele (kleine) online banken die met afgeleide identificatie werken en de thuiswinkelbranche waarbij strikte identificatievaststelling snel leidt tot een daling in de verkoop.
Private partijen compenseren voor de geleden financiële schade wanneer op grond van onderzoek blijkt dat er sprake is van identiteitsfraude.
Doorverwijzing van slachtoffers naar meldpunten, zoals het CMI, lijkt in de private sector minder gebruikelijk dan in de publieke sector.
Binnen de private sector bestaat behoefte om onderling kennis en ervaringen uit te wisselen, samen te werken met onder meer de politie en de instelling van een database met daarin de gegevens van bevestigde fraudeurs.

6 Inzet overige betrokken partijen

Naast de organisaties waar de fraude heeft plaatsgevonden, kunnen slachtoffers in contact komen met de politie en hulpverlenende organisaties. Dit hoofdstuk behandelt eerst de inzet van de politie en vervolgens enkele hulpverlenende organisaties (CMI, Fraudehelpdesk, Slachtofferhulp Nederland en Nationale Ombudsman). Het hoofdstuk sluit af met een korte beschrijving van fondsen die slachtoffers compenseren voor geleden schade (door andere delicten dan identiteitsfraude).

6.1 Inzet politie

Aangifte cruciaal voor slachtoffers

De rol van de politie in het huidige onderzoek is meervoudig, maar één ervan is het opnemen van aangiftes. De aangifte is voor de politie nodig om onderzoek te kunnen doen en voor het slachtoffer belangrijk in het herstel- en compensatieproces richting andere organisaties. Uitvoeringsorganisaties, en in sommige gevallen ook private organisaties, hanteren namelijk als voorwaarde voor hulp dat het slachtoffer bij de politie aangifte doet van identiteitsfraude. Zoals in paragraaf 3.4 gemeld, doet echter slechts een beperkt deel van de slachtoffers aangifte van identiteitsfraude.

Tot voor kort konden slachtoffers niet altijd aangifte doen

Uit het beeld dat geschetst is door de verschillende organisaties blijkt dat tot een paar jaar geleden aangiftes bij de politie niet of nauwelijks opgenomen werden. Men had moeite om het strafbare feit juridisch te duiden. Het 'jezelf uitgeven voor een ander' was namelijk tot april 2014 niet strafbaar, het delict waarvoor iemands identiteit werd gebruikt, was dat wel. De aangifte diende te worden opgetekend onder valsheid in geschifte of oplichting. De politie verwees daardoor over het algemeen naar civiele procedures. En in de beleving van het slachtoffer werd men regelmatig weggestuurd, men kreeg 'nul op rekest'[30]. Naast moeite met de juridische duiding was ook werkdruk een oorzaak voor het niet opnemen van een aangifte. In het interview met medewerkers van de politie werd dit beeld bevestigd.

Grote verbeteringen in de frontoffice van de politie

Volgens de politie zelf en een aantal overheidsorganisaties zijn er grote verbeteringen geweest in de frontoffice van de politie, waardoor aangiftes nu vaker dan voorheen worden opgenomen. Een belangrijke reden daarvoor is de strafbaarstelling van identiteitsfraude als delict op zichzelf in april 2014 (artikel 231b Wetboek van Strafrecht). Ook is er volgens de politie intern toenemende aandacht voor het fenomeen identiteitsfraude[31] en zijn medewerkers alerter op de mogelijke gevolgen van diefstal van identiteiten. Daarnaast besteedt politie aandacht aan de aanpak van identiteitsfraude en het belang van een goede identiteitsvaststelling bij de huidige uitrol van MEOS en zal de interne opleiding bij de uitrol van een ICT-applicatie, BV-ID 2.0, begin 2016, ook hiervoor benutten. Ook richt de politie per eenheid een herkenbaar 'loket' in met ID onderzoekers[32] en zijn er met het CMI afspraken gemaakt over de bemiddeling van slachtoffers wanneer zij bij het CMI aangeven geen aangifte te kunnen doen of als men geen aangifte heeft gedaan.

---

[30] Zie onder andere: Genova, *Komt een vrouw bij de h@cker*, en Nationale Ombudsman, *Herzien openbaar rapport, rapportnummer 2009/199*.

[31] Identiteitsvaststelling in de strafrechtketen heeft in zijn algemeenheid meer aandacht gekregen.

[32] Deze loketten maken onderdeel uit van de Afdeling Vreemdelingenpolitie, Identificatie en Mensenhandel (AVIM), de operationele afdeling voor o.a. identiteitsfraude.

Ondanks deze maatregelen gaat het doen van aangifte in geval van identiteitsfraude nog niet in alle gevallen goed, aldus de politie. Er is echter wel een positieve ontwikkeling ingezet. Het CMI merkt dat de laatste tijd minder klachten binnen komen over 'niet opgenomen aangiftes'. Andere overheidsorganisaties melden eveneens dat het aantal slachtoffers dat bij hen terugkomt omdat het niet lukt om aangifte te doen, de afgelopen jaren geleidelijk afneemt.

Deze ontwikkelingen in de aangifte-mogelijkheden voor slachtoffers lijken ook nodig. Een aantal organisaties, met name de private partijen, zijn niet onverdeeld positief over de mogelijkheden voor slachtoffers om aangifte te doen. Daarnaast hebben zij de indruk dat identiteitsfraude nog steeds laag op de hiërarchische ladder van strafbare feiten staat en dat opsporing geen prioriteit heeft; er is niet de urgentie van een inbraak/overval of de schade van een geweldsmisdrijf.

Slachtoffer kan ook dader zijn

Binnen de politie bestaat een waakzame houding tegenover beweringen van identiteitsfraude, omdat een meegaande houding ook kwaadwillende figuren in de kaart kan spelen. Er moet bovendien sprake zijn van enig nadeel, maar wat dat nadeel in een identiteitsfraude is, valt bij aangifte lang niet altijd aan te wijzen. Dat kan aanleiding zijn tot twijfel bij de politie waardoor een aangifte niet altijd direct wordt opgenomen.

LMIO onderzoekt grootschalige zaken

Het LMIO, de expertafdeling binnen de politie die zich met name bezighoudt met aankoop- en verkoopfraude, onderzoekt grootschalige fraudezaken. De meldingspagina van het LMIO op www.politie.nl vraagt om die reden gegevens van het slachtoffer en zoveel mogelijk informatie over de dader. Het blijkt dat meerdere slachtoffers vaak de dezelfde dader kennen. Het LMIO geeft na een melding via een e-mail een aantal tips aan het slachtoffer (aangifte, nieuw ID-bewijs aanvragen), maar behandelt feitelijk niet het individuele geval (door een onderzoek in te stellen). Na tien weken ontvangt het slachtoffer bericht over wat er met de melding is gebeurd (in de meeste gevallen is de melding niet voor verder onderzoek opgepakt binnen die termijn en wordt de zaak gesloten). Daarnaast informeert LMIO na vijf meldingen over een rekeningnummer banken over deze verdachte rekeningnummers.

ECID helpt bij vastgelopen identiteitsfraudezaken

Het Expertisecentrum Identiteitsfraude en -documenten (ECID) geeft voorlichting en advies aan overheden en politie en helpt bij identiteitsfraude. De Koninklijke Marechaussee en politie werken samen in het ECID. Het ECID treedt op als politieonderzoek stokt en/of als het CMI aangeeft dat er in een zaak sprake is van identiteitsfraude. In een dergelijk geval voert het ECID vanuit de eigen expertise onderzoek uit. Zij nemen in dat geval ook de communicatie met de politie op zich. Medewerkers van het ECID treden in contact met het desbetreffende politiekorps, kijken naar de status van het onderzoek, checken de feiten en delen nieuwe informatie met het regionale korps. Het rechtzetten van de schade en het opsporen van de dader, met andere woorden genoeg doening, is voor het ECID een belangrijke factor.

Volgens het ECID is de samenwerking binnen de identiteitsketen nog niet voldoende. De samenwerking tussen politie, marechaussee en OM wordt wel beter. Het ECID stelt een betere coördinatie van de handhavingsaanpak rondom identiteitsfraude voor en regelmatige controles of de keten afdoende functioneert of dat aanpassingen wenselijk zijn.

Informatiebeheer politie-/justitieketen soms nadelig voor slachtoffers

Voor politie en justitie is het van belang dat de identiteit correct wordt vastgesteld. Pas daarna wordt gekeken naar de rol van de persoon (bijvoorbeeld of hij een strafbaar feit heeft gepleegd, verdachte is, veroordeelde, of slachtoffer van een misdrijf) en wat er aan dienstverlening nodig is. Vingerafdrukken maken binnen het straf- en vreemdelingenrecht deel uit van de identificerende gegevens van een persoon[33]. Doordat de vingerafdrukken in de informatiesystemen van de politie en justitieketen zijn geregistreerd en in de verschillende processen worden gecontroleerd is identiteitsverwisseling binnen een strafproces nagenoeg uitgesloten. De Matching Autoriteit bewaakt de identiteit in deze processen. Daarmee kan bijvoorbeeld worden voorkomen dat een persoon onder dwang of misschien tegen betaling een gevangenisstraf voor een ander uitzit. Het kan evenwel nog wel voorkomen dat identiteitsfraude aan de voorkant van het proces (dus bij eerste identificatie) voorkomt.

Naast de basissystemen (zoals Basisvoorziening voor vreemdelingen en Strafrechtketendatabase), zijn er in de politieorganisatie nog tal van andere informatiesystemen in gebruik. Door het ontbreken van een beheerregistratie (een overzicht van alle in gebruik zijnde informatiesystemen binnen de politie) is het volgens de politie moeilijk om volledig te voldoen aan een verzoek tot verwijdering van persoonsgegevens uit 'de politieregisters' (zie de zaak Kowsoleea). Anders gezegd, een slachtoffer van identiteitsfraude kan zich voor het probleem gesteld zien, dat zijn gegevens steeds weer opduiken in een van de politieregistraties die niet is opgeschoond. De politie maakt een uniforme landelijke werkinstructie waarin onder meer staat welke informatiesystemen van de politie gecontroleerd en dus geschoond moeten worden als er sprake is van een persoonsverwisseling.

[33] Er zijn in de Wet op de inlichtingen en veiligheidsdiensten strikte regels opgenomen over wanneer vingerafdrukken mogen worden afgenomen.

6.2 Hulporganisaties

6.2.1 Het Centraal Meldpunt Identiteitsfraude en -fouten

Het CMI staat slachtoffers gedurende het proces van melding en herstel bij met advies en begeleiding. Ze bemiddelt tussen overheidsinstanties, private partijen en het slachtoffer, om registraties gecorrigeerd en/of schade hersteld te krijgen.

Online melding via het CMI

Slachtoffers van identiteitsfraude kunnen op de website van het CMI een formulier invullen waarop zij de melding doen, waarbij zij een beschrijving geven van de fraude (onder andere het middel, de methode van diefstal, de gerealiseerde fraude en de schadeomvang). Het CMI neemt vervolgens telefonisch contact op met het slachtoffer om te analyseren wat er precies gebeurd is. Het CMI streeft ernaar met het slachtoffer een goed dossier samen te stellen, inclusief bijvoorbeeld de aangifte die bij de politie is gedaan.

Begeleiding bij herstel

De naam meldpunt is eigenlijk te beperkt. Het CMI helpt het slachtoffer namelijk ook met het beëindigen en herstellen van de identiteitsfraude. Slachtoffers van identiteitsfraude kunnen te maken krijgen met het welbekende kastje-muur verhaal, bijvoorbeeld als private partijen niet de vorderingen van iemands naam willen halen en de politie meldt dat er geen aangifte gedaan kan worden.

In dergelijke gevallen informeert het CMI slachtoffers over zijn/haar rechten en geeft advies op maat.

Het CMI heeft de afgelopen jaren bij diverse (overheids)instanties een ingang weten te creëren. De burgers die bijvoorbeeld op enige wijze zijn gedupeerd via de systemen van de Belastingdienst worden via deze ingang ‘intern uitgezet’ bij de Belastingdienst en verder onderzocht. Het CMI geeft aan dat hun rol daarbij vrij cruciaal is, omdat burgers er zelf bij publieke en private partijen vaak niet doorheen komen; men krijgt dan nul op rekest bij de eerstelijnsdienstverlening (klantcontactcentrum, klantenservice, et cetera).

De contacten van het CMI bij private partijen zijn beperkt. Het CMI moet momenteel zelf ook wel eens met de klantenservice bellen, maar geeft aan daarmee meer gedaan te krijgen dan een individuele burger. De komende periode wil het CMI investeren in de relaties met private partijen, zodat ze daar (nog) beter als bemiddelaar kunnen fungeren.

Luisterend oor

Een ander belangrijk element in de dienstverlening van het CMI bestaat uit het bieden van een luisterend oor. Het CMI helpt een slachtoffer zijn/haar verhaal helder te krijgen en luistert zonder daarbij een standpunt in te nemen, zoals sommige andere organisaties – vanuit hun verantwoordelijkheden – wel doen. Denk bijvoorbeeld aan de politie die eerst zeker wil weten met een slachtoffer en niet een dader van identiteitsfraude van doen te hebben. Net als andere hulpverlenende organisaties merkt het CMI op dat slachtoffers veel behoefte hebben aan erkenning en begrip, zoals dit ook geldt voor slachtoffers van (gewelddadige) misdrijven.

Actief als ketenregisseur

Het CMI voert met diverse organisaties, zoals de Belastingdienst, RDW, Politie, ECID, IND, Matchingsautoriteit en Logius regelmatig ketenoverleg, waarbij het CMI ketenregisseur is. In dit overleg worden trends gesignaleerd, individuele casussen gezamenlijk besproken en afspraken gemaakt over samenwerking.

De meeste partijen vinden het ketenoverleg nuttig en zijn van mening dat meer partijen deel zouden moeten nemen. Zij denken daarbij aan uitbreiding met private partijen, omdat daar de meeste fraude plaatsvindt. Private partijen onderschrijven het nut van overleg tussen de publieke en private organisaties, met name op het vlak van fraudebestrijding.

Met de ketenpartners uit het ketenoverleg is een arrangement gesloten, waarin afspraken zijn opgenomen over hoe meldingen van identiteitsfraude dienen te worden afgehandeld[34]. Met de Belastingdienst, RDW, ECID en de politie zijn daarnaast nog specifieke werkafspraken gemaakt. De politie stuurt aangiften door naar de ECID die kijkt of zaken opgeplust moeten worden en daardoor meer prioriteit krijgen.

Bekendheid van het CMI

Met name de publieke organisaties zijn bekend met het CMI. De meeste publieke organisaties hebben korte lijnen met het meldpunt en adviseren slachtoffers zich daar ook te melden. In de private sector zijn vrijwel alle geïnterviewde organisaties bekend met het bestaan van ‘een centraal meldpunt voor identiteitsfraude’, maar niet met het CMI. Zij verwijzen dan ook in de regel niet door naar het CMI; de rol

[34] Arrangement ketenpartners en Centraal Meldpunt Identiteitsfraude en -fouten

van het meldpunt is ook niet voor alle private partijen helder. Uit de gesprekken blijkt tevens dat de partijen de landelijke (naams)bekendheid bij de *burger* nog gering vinden.

Beeld van het CMI vanuit de publieke sector

Het CMI heeft volgens de geïnterviewde publieke organisaties de laatste jaren veel meters gemaakt. Het is een organisatie in ontwikkeling die zijn rol binnen de identiteitsketen op steeds meer plekken vormgeeft. In zeer korte tijd is het CMI, volgens een aantal van de uitvoeringsorganisaties, behoorlijk onmisbaar geworden. De lijnen met publieke organisaties worden steeds korter door structureel ketenoverleg en de vele op incidenten gestoelde samenwerkingsverbanden met medewerkers van diverse organisaties in de publieke sector. De contacten met het CMI worden dan ook als zeer goed omschreven. Publieke instanties krijgen vrijwel nooit slachtoffers die zich opnieuw bij hen melden omdat het CMI ze niet kon helpen. Wel zou volgens justitie en politie een beetje gezonde achterdocht geen kwaad kunnen bij de benadering van het slachtoffer, omdat er ook daders tussen kunnen zitten.

Een aantal partijen geeft aan dat het CMI in hun beleving niet altijd genoeg slagkracht of mandaat heeft om alle slachtoffers goed te kunnen helpen wanneer bemiddeling of interventies door het CMI nodig zijn. Hierdoor zouden zaken soms lang op de plank liggen. Het CMI geeft aan dat er eerder inderdaad sprake was van een vrij lange doorlooptijd, maar dat in 2015 de wachttijd is verkort tot twee à drie weken en spoedgevallen vrijwel direct worden opgepakt. Sommige meldingen hebben een lange doorlooptijd door de aard van de melding of omdat er bij een reeds afgeronde melding opnieuw sprake is van fraude. De formatie is naar eigen zeggen voldoende voor de gestelde taken.

Beeld van het CMI vanuit private sector

Hoewel we onvoldoende private partijen gesproken hebben om een betrouwbare uitspraak te doen voor de hele private sector, bestaat het beeld dat het CMI geen grote bekendheid geniet in de sectoren. Opvattingen over het CMI zijn bij geïnterviewde partijen soms ook gebaseerd op ervaringen van een paar jaar terug. De partijen in kwestie twijfelen over de mogelijkheden van het CMI, ofwel de invloed die het CMI heeft mede vanwege het ontbreken van een link met justitie. Deze opvattingen over het CMI laten zien dat private partijen niet zo maar de samenwerking met het CMI zoeken en slachtoffers die zich bij hen melden naar het CMI doorverwijzen.

De meeste geïnterviewde private partijen hebben wel behoefte aan direct contact en samenwerking met een hulpverlenende instantie omdat zij in sommige gevallen het slachtoffer niet kunnen helpen (of omdat er signalen zijn dat de schade voor het slachtoffer groter is dan bij hun bedrijf alleen).

6.2.2 Fraudehelpdesk

De Fraudehelpdesk is een stichting die, mede dankzij subsidie van het Rijk, advies en (juridische) ondersteuning biedt aan slachtoffers van fraude in brede zin (acquisitiefraude, datingfraude, identiteitsfraude, et cetera). De stichting probeert burgers en bedrijven te behoeden voor oplichtingspraktijken door hen bewust te maken van de risico's en hen te wijzen op preventieve maatregelen.

Fraudehelpdesk zet meldingen door naar CMI en geeft advies

De Fraudehelpdesk heeft met het Ministerie van BZK de afspraak gemaakt de particuliere melders van identiteitsfraude door te verwijzen naar het CMI, wat de stichting naar eigen zeggen ook doet. Naast het doorverwijzen naar het CMI, verwijst de stichting slachtoffers soms door naar een juridisch loket of naar de eigen juridische adviseurs. Daarnaast raadt de stichting slachtoffers aan om aangifte te doen.

De Fraudehelpdesk is van mening dat de burger met een doorverwijzing naar het CMI weinig opschiet, vooral wanneer de fraude is ontstaan bij een private partij. Slachtoffers moeten dan vaak zelf het gesprek aangaan met de private partij. De Fraudehelpdesk wil meer mandaat krijgen om voor slachtoffers zaken te regelen.
De Fraudehelpdesk pleit voor een fonds waarmee slachtoffers van identiteitsfraude kunnen worden gecompenseerd voor de geleden (financiële) schade.
Daarnaast wil de Fraudehelpdesk dat informatie van het CMI vaker aan hen wordt doorgegeven. Door versnippering van informatie tussen allerlei instanties, duren zaken volgens de Fraudehelpdesk onnodig lang. Het CMI geeft echter aan dat wanneer een burger zich meldt bij beide organisaties, er ad hoc overleg plaatsvindt tussen de beide organisaties, zodat het slachtoffer zich niet twee keer hoeft aan te melden.

Een publiek- en een privaatgerichte hulporganisatie

De Fraudehelpdesk is van mening dat de begeleiding van slachtoffers van identiteitsfraude op papier aardig is uitgewerkt, maar dat in de praktijk slachtoffers regelmatig tussen wal en schip vallen. De Fraudehelpdesk pleit om die reden voor het ontwikkelen van een model waarin er een partij komt die meer mandaat krijgt en de regie neemt. Voor de publieke sector zou dat het CMI moeten zijn, maar richting private partijen heeft de Fraudehelpdesk in haar optiek betere contacten.

Het CMI geeft aan dat de huidige verdeling in principe houdbaar is. De Fraudehelpdesk behandelt meerdere vormen van fraude en heeft goede contacten in het private domein. Het CMI richt zich enkel op identiteitsfraude en heeft de noodzakelijke contacten in het publieke domein. Indien haar bekendheid bij private (en sommige publieke) organisaties verbetert, kan het CMI – dankzij haar specialistische kennis en ervaring op het terrein van identiteitsfraude – ook deze sector uitstekend bedienen.

6.2.3 Slachtofferhulp Nederland

Slachtofferhulp Nederland helpt slachtoffers met praktische, juridische en psychosociale ondersteuning. Het gaat hierbij om directe hulpverlening voor mensen die even uit het lood zijn geslagen. Slachtoffers melden zich zelf bij Slachtofferhulp Nederland. Ook komt het voor dat de politie gegevens van slachtoffers aan de hulpdienst verstrekt. Afhankelijk van het exacte delict en wat het slachtoffer wil, bieden ze ondersteuning en advies op praktisch, emotioneel en juridisch vlak.

Het valt Slachtofferhulp Nederland op dat de behoeften van slachtoffers van identiteitsfraude niet wezenlijk anders zijn dan van slachtoffers van andere delicten (geweld, roof, misbruik, et cetera). In beide gevallen is er sprake van verdriet en boosheid en schaamte om te vertellen wat er is gebeurd. Slachtofferhulp Nederland heeft de ervaring dat slachtoffers van identiteitsfraude door betrokken partijen (en door hun omgeving) niet altijd als slachtoffer worden behandeld, zoals dat bij geweldsdelicten wel gebeurt.

Om de situatie voor slachtoffers te verbeteren stelt Slachtofferhulp Nederland dat het bieden van ondersteuning aan slachtoffers van groot belang is en dat slachtoffers – meer dan nu het geval is – gewezen moeten worden op de mogelijkheid van herstelrecht.

Nog geen (formele) relatie met het CMI

De relatie tussen slachtofferhulp en het CMI moet nog worden ontwikkeld. Slachtofferhulp Nederland geeft aan dat structureel contact zinvol kan zijn, omdat burgers die last hebben van identiteitsfraude juist behoefte hebben aan (persoonlijk) contact om hun verhaal te doen. Slachtofferhulp Nederland zou daarom graag in contact treden met het CMI. Of er door de frontoffice van Slachtofferhulp Nederland wordt doorverwezen naar het CMI kon de organisatie niet mededelen. Gegevens over de doorverwijzing worden niet in die mate van detail geregistreerd.

6.2.4 De Nationale Ombudsman

De Nationale Ombudsman intervenieert en bemiddelt voor slachtoffers richting overheidsinstanties. Wanneer de Nationale Ombudsman een zaak oppakt, dan wordt deze vaak veel sneller afgehandeld dan wanneer een burger zelf probeert de schade te herstellen. De zaak Kowsoleea is feitelijk de eerste keer dat een zaak van identiteitsfraude groot door de Ombudsman werd opgepakt.

De Nationale Ombudsman vindt het belangrijk om slachtoffers bij te staan bij het herstel in de identiteitsketen. De Ombudsman biedt dan ook begeleiding en hulp wanneer het slachtoffer zich eerst heeft gemeld bij de overheidsinstantie waar de fraude heeft plaatsgevonden. De Ombudsman is mediator richting overheidsinstellingen. Met de meeste overheidsinstellingen onderhoudt de Ombudsman – naar eigen zeggen – goede contacten. Met het CMI heeft de Ombudsman (nog) geen contact, wel verwijst de Ombudsman naar deze organisatie door wanneer er sprake is van identiteitsfraude.

De Nationale Ombudsman vindt dat het slachtofferperspectief tot nu toe onderbelicht is geweest in het beleid rondom identiteitsfraude. Volgens de Ombudsman is het belangrijk dat slachtoffers zo snel mogelijk schadeloos worden gesteld, zoals sommige overheidsinstellingen reeds doen. In elk geval zal bij elke individuele casus gecontroleerd moeten worden of het slachtoffer financiële problemen heeft of als gevolg van de identiteitsfraude kan krijgen. De Ombudsman spreekt daarbij de voorkeur uit dat schadeloosstelling gebeurt door de betrokken instanties gezamenlijk.
Ook moet de overheid volgens de Nationale Ombudsman in geval van identiteitsfraude (meer) verantwoordelijkheid nemen voor het opschonen van systemen en bij signalen/meldingen van identiteitsfraude op individueel niveau controleren of bestanden wel correct zijn gekoppeld. En tot slot moet de overheid daadwerkelijk gebruik maken van alle veiligheidscontroles die overheidsinstanties wettelijk gezien zouden moeten gebruiken.

6.3 Geen compensatie door fondsen

Meldpunten en hulpverlenende organisaties begeleiden slachtoffers in het proces tot herstel van hun identiteit, fondsen kunnen een bijdrage leveren bij het compenseren voor eventuele financiële schade. Er zijn twee publieke fondsen die compensatie bieden aan slachtoffers van misdrijven: de eerste is het Schadefonds Geweldsmisdrijven, de tweede het Waarborgfonds Motorverkeer. Beiden zijn niet toegankelijk voor slachtoffers van identiteitsfraude. De volgende beschrijving van de fondsen kan worden benut indien in het geval van identiteitsfraude aan een fonds wordt gedacht.

Schadefonds Geweldsmisdrijven
Het Schadefonds Geweldsmisdrijven keert uit aan slachtoffers van een geweldsmisdrijf of nabestaanden. De uitkering is bedoeld als smartengeld en als tegemoetkoming in medische kosten en gederfde inkomsten. Het schadebedrag is afhankelijk van de letselcategorie waar het slachtoffer in valt en varieert tussen de € 1.000 en € 35.000. De letselcategorie wordt op basis van het dossier bepaald door medisch adviseurs, die zo nodig navraag doen bij behandeld artsen of psychologen. De belangrijkste criteria om hiervoor in aanmerkingen te komen, zijn:

- Het geweld moet opzettelijk gebruikt zijn, blijkend uit bijvoorbeeld de aangifte bij de politie.
- Er is sprake van ernstig fysiek of psychisch letsel.
- Het letsel is langdurig of blijvend.
- Het misdrijf is in Nederland gepleegd.
- Het slachtoffer heeft het misdrijf niet veroorzaakt of er aandeel in gehad.

De afhandeling van aanvragen duurt ongeveer 26 weken, aldus de website. Het fonds krijgt jaarlijks ongeveer 7.000 aanvragen. Tegenover elke 6 toegekende aanvragen stonden 4 afwijzingen. De gemiddelde uitkering was in 2014 € 3.161.

Waarborgfonds Motorverkeer
Het Waarborgfonds Motorverkeer vergoedt schade van personen door een aanrijding van een motorvoertuig. Het gaat dan om schade aan de eigen auto, letselschade of schade aan andere materiële zaken (huis, fiets, et cetera). Het fonds keert uit als de veroorzaker onbekend of onverzekerd is. De voor dit rapport belangrijkste criteria zijn:

- Het slachtoffer moet getracht hebben de dader te achterhalen (door bijvoorbeeld aangifte bij de politie of navraag bij omwonenden te doen).
- De schade moet door een motorvoertuig zijn veroorzaakt (bewijslast).

Het fonds kreeg de afgelopen jaren volgens hun jaarverslag ongeveer 50.000 claims per jaar binnen. Het toekenningspercentage ligt op 77%. Het gemiddeld uitgekeerde bedrag is volgens onze eigen schatting op basis van de cijfers in het jaarverslag ongeveer € 1.500.

6.4 Conclusies

De politie speelt een belangrijke rol waar het gaat om het afwikkelen van een identiteitsfraudezaak. Het doen van aangifte is vaak cruciaal voor slachtoffers om de directe financiële schade van de fraude vergoed te krijgen. Aanvankelijk kwam het voor dat de politie geen aangifte opnam wanneer er sprake was van identiteitsfraude. Tegenwoordig verloopt dit proces beter, al zijn er volgens de politie nog verbeteringen mogelijk. Dit geldt ook voor de registratie van persoonsgegevens binnen de politie. Het verwijderen van deze gegevens in de databases van de politie blijft een punt van aandacht
Naast de politie spelen ook hulpverlenende organisaties een belangrijke rol. Het CMI begeleidt slachtoffers van identiteitsfraude en vervult de rol van ketenregisseur binnen de publieke sector, binnen de private sector is haar netwerk minder uitgebreid. Verbeteringen zijn mogelijk waar het gaat om het begeleiden van slachtoffers binnen de private sector en waar het gaat om het verbinden van expertise uit de publieke en private sector.
Er zijn geen fondsen die slachtoffers van identiteitsfraude schadeloos stellen.

Deel C: Juridische verkenning van mogelijkheden voor compensatie van slachtoffers

7 *Juridische mogelijkheden voor compensatie*

In deel B stond de feitelijke omgang met slachtoffers van identiteitsfraude centraal. Daaruit bleek dat alle geïnterviewde overheidsinstanties overgaan tot compensatie van directe schade zodra de burger voldoende aannemelijk maakt slachtoffer te zijn geworden van identiteitsfraude en eventueel aangifte heeft gedaan.

In dit hoofdstuk wordt het vraagstuk van compensatie en schadevergoeding nader juridisch geduid. Daarbij zullen wij bespreken wat de reikwijdte is van de juridische verplichting om de gevolgen van ID-fraude ongedaan te maken en (eventueel) de daaruit voortvloeiende schade te vergoeden, bij gebreke waarvan het handelen van de overheid onrechtmatig wordt. Na een uiteenzetting van de onderzoeksvragen en de verantwoording van het juridische onderzoek, geeft dit hoofdstuk een samenvatting van de verkenning. De integrale tekst vindt u in een aparte bijlage (Bijlage C).

7.1 Onderzoeksvragen en verantwoording van de juridische verkenning

De juridische verkenning richt zich op een vergelijking tussen de wijze waarop private respectievelijk publieke organisaties omgaan met de nadelige gevolgen van ID-fraude. Om deze vergelijking te kunnen maken, is het onontbeerlijk om inzicht te hebben in het relevante juridische kader. Daartoe worden twee hoofdthema's belicht: enerzijds de *ongedaanmaking* van de nadelige gevolgen van identiteitsfraude en anderzijds de voorwaarden waaronder de overheid en private partijen *aansprakelijk* kunnen worden gesteld voor de (overige) gevolgen van identiteitsfraude. Bij de ongedaanmaking van nadelige gevolgen kan het zowel om financiële als om niet-financiële gevolgen gaan. Bij financiële gevolgen valt te denken aan de terugvordering van bedragen die nooit aan het slachtoffer zijn uitgekeerd; bij niet-financiële gevolgen kan worden gedacht aan het herstel van onjuiste registraties in basisregistraties. Bij de aansprakelijkheidsvraag gaat het per definitie om op geld waardeerbare schade: denk aan verminderde inkomsten in de vorm van gemiste opdrachten door een slechte reputatie. Deze schade kan zowel materieel zijn (gederfde inkomsten bijvoorbeeld) als immaterieel (onrust, stress, et cetera) zijn.

De reden om ook het eerstgenoemde thema te belichten is dat het slachtoffer van identiteitsfraude als regel niet zal beginnen met een aansprakelijkheidsstelling, maar eerst en vooral zal trachten de ID-fraude ongedaan te maken. De uitkomst van dat traject kan een rol spelen bij een eventuele aansprakelijkstelling, zoals wij nog zullen toelichten.

Samenvattend staan in de juridische verkenning de volgende twee hoofdvragen centraal:

1. Onder welke juridische voorwaarden kan een slachtoffer van ID-fraude zorgen voor ongedaanmaking van de gevolgen van ID-fraude in zowel de publieke als de private sector?

2. Onder welke juridische voorwaarden kan een slachtoffer van ID-fraude schadevergoeding verkrijgen van rechtssubjecten in zowel de publieke sector als de private sector?

Om in aanmerking te komen voor vergoeding van schade of de ongedaanmaking van de gevolgen van identiteitsfraude door een overheidsinstelling, moet allereerst worden vastgesteld wat de betrokkenheid van de overheid bij de identiteitsfraude is. Een blik op de jurisprudentie leert dat er niet veel voorbeelden zijn van (succesvolle) aansprakelijkstellingen van de overheid, waarbij de vergoeding van schade de directe inzet van het geschil was. Geschillen ontstaan reeds in situaties dat een overheidsinstelling een nadelig besluit niet wenst te herzien na een beroep op vermeende identiteitsfraude door de burger. Hierbij kan gedacht worden aan procedures die bij de bestuursrechter worden aangespannen tegen besluiten tot terugvordering van – bijvoorbeeld – ten onrechte verleende, maar beweerdelijk nooit ontvangen, bijstand of uitkering. Ongedaanmaking van dit besluit levert het slachtoffer reeds geheel of gedeeltelijke rechtsherstel op. Ook kunnen procedures ontstaan omdat een onjuist gegeven in een basisregistratie blijft opgenomen. Gelet op de verschillende situaties in de jurisprudentie kan de betrokkenheid van de overheid volgens ons vanuit drie situaties of 'rollen' juridisch worden onderzocht:

1) de betrokkenheid van de overheidsinstelling als *beslissingsbevoegde* bij materieel benadelende beschikkingen;
2) de betrokkenheid van de overheidsinstelling als *verantwoordelijke voor basisregistraties* en de bij haar geregistreerde gegevens;
3) de betrokkenheid van de overheidsinstelling als *aangesprokene* voor anderszins geleden schade.

Bij de situaties 1 en 2 staat het ongedaan maken van de nadelige gevolgen van identiteitsfraude centraal, bij situatie 3 het verhalen van resterende directe of indirecte schade als gevolg van identiteitsfraude. De situaties 1 en 2 komen in het bijzonder tot uiting in procedures bij de bestuursrechter. Situatie 3 komt in de regel tot uiting in een procedure bij de civiele rechter op grond van een actie uit onrechtmatige daad (artikel 6:162 BW) of een meer specifieke aansprakelijkstelling.

Vertalen we de drie situaties naar de twee hierboven geformuleerde hoofdvragen, dan kunnen de twee hoofdvragen worden gesplitst in de volgende deelvragen:

A. Ongedaan maken gevolgen identiteitsfraude (hoofdvraag 1)

A1. Hoe gaat de bestuursrechter om met een beroep op identiteitsfraude bij burger belastende besluiten? Bij wie, en in welke mate, ligt de bewijslast dat het besluit is gebaseerd op onjuiste of op onjuist gebruikte gegevens?

A2. Hoe gaat de burgerlijke rechter om met een beroep op identiteitsfraude bij de nakoming van (ongevraagde) verbintenissen? Bij wie, en in welke mate, ligt de bewijslast als de verwerende partij zich op het standpunt stelt zelf nooit een verbintenis te zijn aangegaan?

A3. Hoe dienen overheidslichamen om te gaan met herstel van fouten in basisregistraties?

A4. In hoeverre wordt (indirecte) schade vergoed door de bestuurs- en de civiele rechter bij een geslaagd beroep op identiteitsfraude in de hiervoor genoemde situaties?

B. Aansprakelijkheid bij identiteitsfraude (hoofdvraag 2)

B1. Kan de overheid naar civiel recht aansprakelijk worden gehouden als een burger slachtoffer wordt van identiteitsfraude?

B2. In hoeverre wordt (indirecte) schade vergoed als de overheid naar civiel recht aansprakelijk kan worden gehouden bij identiteitsfraude?

Een antwoord op deze vragen geeft een juridisch kader voor de mogelijkheden tot herstel en compensatie wanneer een burger zich tot de overheid wendt met de mededeling dat hij slachtoffer is geworden van identiteitsfraude. Daarbij is het juridische kader voor de overheid, waar relevant, vergeleken met het kader rond de omgang met identiteitsfraude door private partijen.

Onderzoeksverantwoording

Om de juridische vragen te beantwoorden zijn de volgende stappen uitgevoerd:

- Analyse wetten en verdragen: Hierbij worden de wetten en verdragen bestudeerd die de wettelijke kaders bepalen voor overheidsaansprakelijkheid en compensatieplichten.
- Analyse wetenschappelijke literatuur.
- Analyse jurisprudentie van zowel nationale rechters als het Europees Hof voor de Rechten van de Mens.
- Vergelijking publiek/privaat: De voorwaarden en regels voor compensatie binnen de private sectoren zijn langs bovenstaande stappen gelegd om duiding te geven aan de verschillen tussen privaatrechtelijk en bestuursrechtelijke aansprakelijkheden en compensatiemogelijkheden/-verplichtingen.

In dit onderzoek is dus niet alleen gekeken naar het nationale kader, maar ook naar de eisen die voortvloeien uit het Europees Verdrag van de Rechten van de Mens (EVRM). Dat verdrag geeft minimumwaarborgen waaraan het nationale kader moet voldoen ten aanzien van de bescherming van mensenrechten. Uit arresten van het Europese Hof voor de Rechten van de Mens (EHRM) volgt dat iemands identiteitsgegevens onder het beschermingsbereik van het EVRM valt. Een analyse van jurisprudentie van nationale rechters en van het EHRM kan dus een beeld geven van de juridische mogelijkheden bij herstel en compensatie in situaties van identiteitsfraude. Op nationaal niveau bespreken we zowel de jurisprudentie van de hoogste bestuursrechters als die van rechtbanken en Hoven. Ook enige relevante literatuur is verwerkt. De strafrechtelijke aansprakelijkheid van de overheid en de herstel- en compensatiemogelijkheden van het slachtoffer in een strafprocedure tegen de fraudeur blijven buiten beschouwing.

Hierna volgt een samenvatting van de juridische verkenning. Eerst wordt gekeken naar de mogelijkheden van *herstel* na identiteitsfraude (onderzoeksvragen A1-4) en daarna naar de mogelijkheden van verdere *vergoeding van (resterende) schade* (onderzoeksvragen B1-2).

7.2 Resultaten

7.2.1 Ongedaan maken gevolgen: onderzoeksvragen A1-4

Bij de ongedaanmaking van de gevolgen van identiteitsfraude door het slachtoffer moeten, zoals hierboven bleek, twee situaties worden onderscheiden. Aan de ene kant de situatie dat het overheidslichaam bij de identiteitsfraude is betrokken doordat het een (positief of negatief) besluit heeft genomen op basis van achteraf onjuist gebleken gegevens. Aan de andere kant de situatie dat het

overheidslichaam bij de identiteitsfraude wordt betrokken als het verantwoordelijk is voor (basis)registraties waarin onjuiste gegevens zijn opgenomen over het slachtoffer van de fraude. Beide situaties kennen, zo blijkt uit de juridische verkenning, een andere maatstaf om te bepalen of ongedaanmaking juridisch verplicht is. Deze verschillen komen hieronder aan de orde.

Ongedaan maken gevolgen benadelende besluiten

Vooropgesteld moet worden dat een overheidsinstelling als beslissingsnemer (‘bestuursorgaan’) zorgvuldig dient te handelen en het nodige onderzoek dient te verrichten voordat het een besluit ambtshalve of op aanvraag neemt. Dit onderzoek gaat echter niet zo ver dat het bestuursorgaan moet controleren of alle gegevens, waaronder de identiteit van de aanvrager, juist zijn. Een bestuursorgaan hoeft daarom, behoudens bijzondere wettelijke voorwaarden of evidente onjuistheden, niet te controleren of een aanvraag voor een begunstigend besluit daadwerkelijk afkomstig is van de persoon op wiens naam de aanvraag staat. Dit gegeven mag worden verondersteld. Deze veronderstelling geldt ook in situaties waarin de aanvraag elektronisch is ingediend na bijvoorbeeld een DigiD-inlogprocedure of een DigiD-elektronische handtekening, tenzij er duidelijke indicaties zijn dat de DigiD-omgeving ten tijde van de aanvraag onvoldoende betrouwbaar was.

Het primaire besluitvormingsproces kent derhalve slechts beperkte juridische verplichtingen om identiteitsfraude op te sporen. Dit betekent echter niet dat het slachtoffer voor een voldongen feit wordt geplaatst. Zodra het slachtoffer op de hoogte raakt van onjuistheden (bijvoorbeeld omdat het post ontvangt over aanvragen die hij nooit heeft ingediend of over besluiten die kennelijk zijn gebaseerd op onjuiste gegevens) is het zaak dat hij zich meldt bij het bestuursorgaan. Weet het slachtoffer aannemelijk te maken dat hij betrokken is bij identiteitsfraude, dan dient het bestuursorgaan het genomen besluit ongedaan te maken.

Bij de ongedaanmaking van de gevolgen van identiteitsfraude ligt de bewijslast en het bewijsrisico bij het slachtoffer. Vanuit het oogpunt van het voorkomen van onterechte beroepen op identiteitsfraude ligt dit voor de hand. Wel is de vraag hoe ver de bewijslast reikt.

Uit het jurisprudentieonderzoek is gebleken dat het slachtoffer bij het bestuursorgaan *aannemelijk dient te maken* dat de gegevens waarop het besluit is gebaseerd onjuist zijn, of bijvoorbeeld niet van hem afkomstig zijn. De invulling van de bewijslast is afhankelijk van alle omstandigheden van het geval. Wel is duidelijk dat een enkele aangifte bij de politie van identiteitsfraude niet voldoende is. Uit de onderzochte jurisprudentie kan worden afgeleid dat het slachtoffer oplettend dient te zijn en adequaat dient te reageren op signalen die op onjuistheden wijzen (zoals brieven of andere signalen). Doet het dat niet en negeert het slachtoffer eerdere signalen die op identiteitsfraude kunnen wijzen, dan verhoogt dat de bewijslast om identiteitsfraude aannemelijk te maken.

In het geval het bestuursorgaan gebruik maakt van gegevens uit een basisregistratie – waarvoor sinds de herstructurering vanaf 2010 een gebruiksplicht bestaat – lijkt de bewijslast voor de burger verzwaard. Het bestuursorgaan beschikt doorgaans niet meer over een controle met gegevens uit een ander register, waaraan een beroep op identiteitsfraude kan worden gespiegeld. Aan de ene kant verhoogt dit de juistheid van de basisregistratie, maar aan de andere kant kan een fout in de basisregistratie sneller op meerdere plaatsen terecht komen. In het kader van de onderzoeksplicht en de zorgvuldigheid

van de besluitvorming mag het bestuursorgaan in de regel zijn besluit baseren op deze gegevens. De drempel om als slachtoffer aannemelijk te maken dat deze centraal opgeslagen gegevens onjuist zijn, lijkt hiermee enigszins verhoogd.

In vergelijking met de civiele rechtspraak valt op dat civiele partijen vaker dienen aan te geven hoe de identificatie van de wederpartij heeft plaatsgevonden. In de civiele rechtspraak lijkt daarmee een strengere lijn te gelden voor de verkopende partij dan in het bestuursrecht voor het bestuursorgaan. Waar het bestuursorgaan in de regel mag aannemen dat de aangeleverde gegevens kloppen, dient een civiele partij – zeker bij online tot stand gekomen overeenkomsten – te controleren of de (vermeende) wederpartij daadwerkelijk de *wil* heeft gehad de overeenkomst aan te gaan. Hoe ver dit onderzoek reikt is niet geheel duidelijk; geautomatiseerde controle via een e-mailadres is bijvoorbeeld mogelijk, maar sluit niet uit dat de fraudeur zelf een e-mailadres op naam van een ander heeft aangemaakt. Bij betwisting van de gesloten overeenkomst door de wederpartij zal de verkopende partij in ieder geval enkele controlestappen hebben moeten verrichten bij de totstandkoming ervan. Op bestuursorganen rust, behoudens bijzondere wettelijke voorschriften en de controle van de methode van elektronische handtekeningen, een dergelijke verplichting niet.

Ongedaan maken onjuiste gegevens in basisregistraties

Tot slot is geconstateerd dat herstel van de gevolgen van identiteitsfraude niet alleen maar plaatsheeft in procedures tegen het materiële benadelende besluit, maar ook in procedures tegen onjuistheden in basisregistraties. De verantwoordelijkheid voor de basisregistratie ligt veelal bij een ander bestuursorgaan dan het bestuursorgaan dat als gebruiker van de registratie het besluit heeft genomen. Dit zorgt ervoor dat het slachtoffer in de systeemketen meerdere procedures zal moeten starten. Opvallend daarbij is dat het rechtsvermoeden dat de gegevens uit de basisregistratie juist zijn, sterk is. In plaats van aannemelijk te maken dat de gegevens onjuist zijn, draagt het slachtoffer bij de aanpassing van onjuiste gegevens de volledige bewijslast. De rechtszekerheid en de betrouwbaarheid van de registratie staat voorop. Alleen als *onomstotelijk vaststaat* dat de in het register opgenomen gegevens onjuist zijn, bestaat een verplichting de gegevens aan te passen. Als dit vervolgens vaststaat, dient de beheerder van het register de aanpassing wel terstond op te nemen als daarmee de kans op verder misbruik wordt voorkomen.

Als het slachtoffer slaagt in het bewijs dat de gegevens onjuist zijn, is vervolgens de hoofdregel dat aanpassing van deze gegevens niet met terugwerkende kracht geschiedt. Dit betekent dat extra procedures over toekomstige materiële besluiten die gebruik maken van historische gegevens niet altijd valt uit te sluiten. Slechts bij hoge uitzondering is aanpassing met terugwerkende kracht mogelijk. Op dit punt geeft de beschikbare jurisprudentie nog geen duidelijk beeld wanneer een uitzondering juridisch moet worden gemaakt. Ook in het geval van aanpassing met terugwerkende kracht zal het slachtoffer verzoeken moeten indienen bij één of meerdere overheidsinstanties om terug te komen op eerdere, onherroepelijke, besluiten genomen op basis van de oude gegevens.

Vergoeding van schade bij ongedaanmaking gevolgen

Uit het jurisprudentieonderzoek is niet gebleken van toegekende schadevergoedingen voor anderszins geleden schade naar aanleiding van onjuiste besluiten. Wel ontvangt het slachtoffer na een procedure bij de rechter een forfaitaire vergoeding van de proceskosten en een vergoeding van de griffierechten.

7.2.2 Aansprakelijkheid: onderzoeksvragen B1-2

Wie de overheid uit onrechtmatige daad wil aanspreken, moet niet te licht denken over zijn succeskansen. Dat geldt ook voor slachtoffers van identiteitsfraude. Wanneer private partijen (banken, telecombedrijven en dergelijke) te maken krijgen met identiteitsfraude, is het over het algemeen niet nodig dat de slachtoffers van die fraude artikel 6:162 BW inroepen om de schade vergoed te krijgen. De mogelijkheid van fraude is veelal verdisconteerd in de algemene voorwaarden, waarbij de betreffende instelling zich verbindt tot het wegnemen van de schadelijke gevolgen van de fraude wanneer de burger zorgvuldig met zijn gegevens is omgegaan en de fraude tijdig heeft gemeld. Krijgen burgers te maken met optreden van overheden waaraan identiteitsfraude ten grondslag ligt, dan lijkt van een dergelijke coulante praktijk geen sprake, zo lijkt althans te volgen uit de door ons bestudeerde bronnen. Weliswaar werd in de uitzonderlijke zaak *Kowsoleea* een coulancecompensatie van 5.000 toegekend euro, maar dit bedrag was lager dan de door het slachtoffer beweerde feitelijk geleden schade. Kortom, de burger dient vooral de traditionele wegen naar aansprakelijkheid te volgen, die ofwel kan rusten op een schending van een wettelijke plicht (zie in het bijzonder de Wet bescherming persoonsgegevens en de Telecommunicatiewet) ofwel kan rusten op artikel 6:162 BW, de algemene actie uit onrechtmatige daad.

Over schending van de in artikel 11 en artikel 13 Wbp opgenomen zorgplichten hebben wij geen relevante rechtspraak gevonden. Ook over artikel 6:162 BW is weinig rechtspraak; wij vonden slechts één vonnis. Dat vrij uitvoerig gemotiveerde vonnis geeft wel een goed inzicht in mogelijke knelpunten waar de gelaedeerde tegen aanloopt. Als degene die stelt dat de overheid onrechtmatig heeft gehandeld rust op hem de plicht om te bewijzen dat de overheid zijn zorgplicht heeft geschonden. De reikwijdte van de op de overheid rustende zorgplichten in de context van identiteitsfraude is nog tamelijk ongewis. Toch hebben wij getracht uit de jurisprudentie een aantal relevante regels af te leiden die, zo menen wij, op overheden evenzeer van toepassing zijn als op bedrijven:

- Burgers moeten worden voorgelicht over de (beveiligings)risico's bij het gebruik van hun product/dienst.
- Als de wijze van fraude verandert en de overheid raakt hiervan op de hoogte, dient het ook onverwijld de voorlichting te veranderen.
- Overheden dienen een juiste administratie bij te houden van de bij hen ingediende aanvragen.

Slaagt de burger erin om te bewijzen dat de zorgplicht is geschonden, dan belanden we in het domein van het schadevergoedingsrecht, en daarin ontmoet de burger nieuwe hobbels. Zo zal hij aannemelijk moeten maken dat hij schade heeft geleden ten gevolge van die schending en dat die schade in een causaal verband staat met het overheidshandelen of –nalaten. Aan de vergoeding van immateriële schade stelt de wet hoge eisen, onder meer door te stellen dat de aansprakelijke partij het oogmerk moet hebben gehad om de schade te veroorzaken. Ten aanzien van de causaliteit speelt het probleem dat het niet eenvoudig is om te bewijzen dat de schade (bijvoorbeeld misgelopen opdrachten) het gevolg waren van het handelen van de overheid dan wel een andere oorzaak hadden, terwijl bij meerdere betrokken overheidsinstellingen elk van deze instellingen apart zal moeten worden aangesproken.

7.3 Besluit

In de inleiding is toegelicht dat rechtsherstel of compensatie voor het

slachtoffer van identiteitsfraude niet alleen betrekking heeft op de aansprakelijkheid van en de schadevergoeding door private en publieke organisaties, maar ook op de mogelijkheden de gevolgen van ID-fraude ongedaan te maken. Immers, ongedaanmaking van de gevolgen gaat als regel aan aansprakelijkstelling (zo die al geschiedt) vooraf. Uit het jurisprudentieonderzoek is in elk geval één opvallend verschil naar voren gekomen. Wanneer een civiele partij (bank, internetverkoper, telecombedrijf) stelt dat een overeenkomst met een wederpartij tot stand is gekomen, draagt hij de bewijslast van het feit dat die wederpartij een overeenkomst heeft *willen* aangaan. Daartoe kan bijvoorbeeld gebruik worden gemaakt van geautomatiseerde e-mailcontrole. Wanneer een burger echter betwist dat gegevens waarop een overheidsbesluit (bijvoorbeeld een besluit tot toekenning van een toeslag) berust juist zijn, draagt hij daarvan de bewijslast en het bewijsrisico. Hij moet alert en proactief reageren vanaf het moment dat de fraude hem bekend kon zijn. Doet hij dat niet, dan kan dat bijvoorbeeld betekenen dat de overheid gelden bij hem kan terugvorderen hoewel de burger zelf beweert die gelden nooit te hebben ontvangen. Bestuursorganen mogen in beginsel vertrouwen op de juistheid van de bij hen aangeleverde gegevens, tenzij er duidelijke contra-indicaties zijn. Met de opkomst van basisregistraties lijkt de bewijslast voor het slachtoffer verder te zijn verzwaard, aangezien er een rechtsvermoeden bestaat dat de

gegevens uit de basisregistratie juist zijn en wijzigingen in de registratie niet licht kunnen worden aangebracht.

Waar het de aansprakelijkheid betreft is het lastig een zuivere vergelijking te maken tussen private en publieke partijen. Zowel voor private partijen als voor de overheid geldt dat de vraag naar de aansprakelijkheid primair wordt bepaald door artikel 6:162 BW. In veel geschillen tussen private partijen wordt niet aan dit artikel toegekomen, aangezien private partijen vaak uit zichzelf tot compensatie overgaan zonder een rechterlijke uitspraak af te wachten. Wanneer de overheid partij is, zal de burger zijn rechtsherstel vooral moeten zoeken door te proberen de nadelige gevolgen van de ID-fraude ongedaan te maken. Als hij erin slaagt de ten onrechte op zijn naam geregistreerde boetes, toelagen of uitkeringen ongedaan gemaakt te krijgen, zal veelal geen andere schade meer resteren. Is dat (uitzonderlijk) toch het geval, dan gelden de gebruikelijke vereisten voor schadevergoeding op grond van een onrechtmatige daad: de wederpartij moet toerekenbaar onrechtmatig hebben gehandeld jegens het slachtoffer, de schade dient bewijsbaar te zijn en de schade dient in een causaal verband te staan met de ID-fraude. Als ongedaanmaking reeds heeft plaatsgevonden, zal slechts in uitzonderlijke situaties ruimte zijn voor (verdere) schadevergoeding, zo er al resterende schade bestaat. Het gebrek aan jurisprudentie op dit punt geeft echter een aanknopingspunt dat slachtoffers deze weg in de praktijk niet bewandelen.

Deel D: Bijlagen

Bijlage A. Afkortingenlijst

AVIM = Afdeling Vreemdelingen, Identificatie en Mensenhandel (onderdeel van de nationale politie)
BKR = Bureau Krediet Registratie
BRP = Basisregistratie Personen (voormalige GBA)
BW = Burgerlijk Wetboek
CBP = College voor Bescherming Persoonsgegevens
CMI = Centraal Meldpunt Identiteitsfraude en –fouten
DUO = Dienst Uitvoering Onderwijs (Ministerie van Onderwijs, Cultuur en Wetenschap)
ECID = Expertisecentrum Identiteitsfraude en Documenten (samenwerking tussen KMAR en de nationale politie)
EVIM = Expertisecentrum Vreemdelingen, Identificatie en Mensenhandel (onderdeel van de nationale politie)
EVRM = Europees Verdrag voor de Rechten van de Mens
GBA = Gemeentelijke Basisadministratie (nu BRP)
IND = Immigratie- en Naturalisatiedienst (Ministerie van Veiligheid en Justitie)
LMIO = Landelijk Meldpunt Internetoplichting (onderdeel van de Nationale Politie)
KMAR = Koninklijke Marechaussee
KNB = Koninklijke Notariële Beroepsorganisatie
KvK = Kamer van Koophandel
NIK = Nederlandse Identiteitskaart
NVB = Nederlandse Vereniging van Banken
OM = Openbaar Ministerie
RDW = Rijksdienst voor Wegverkeer
SVB = Sociale Verzekeringsbank

TIF = Team identiteitsfraude (gemeente Amsterdam)
UWV = Uitvoeringsinstantie Werknemersverzekeringen (Ministerie van Sociale Zaken en Werkgelegenheid)
WODC = Wetenschappelijk Onderzoek- en Documentatiecentrum (Ministerie van Veiligheid en Justitie)
VIS = Verificatie Informatie Systeem

Bijlage B Bronnen voor literatuurstudie

Auteurs en titel	Korte beschrijving
Grijpink, J.H.A.M., 'Identiteitsfraude en overheid' in: *Justitiële verkenningen*, jaargang 32, nr. 7 2006.	Het artikel geeft inzicht van het beleid van de overheid m.b.t. identiteitsbewijzen en de bestrijding van fraude. Grijpink stelt dat het gekozen spoor van de overheid (op het gebied van bestrijding) juist de dader in plaats van het slachtoffer helpt. Door standaardiseren en versimpelen van persoonsgegevens en ID-bewijzen is het voor de daders makkelijker om te frauderen. Grijpink pleit voor meer sectorale identiteitsgegevens aan de preventiekant en een laagdrempelig instituut (het CMI) waar burgers zich kunnen melden bij identiteitsfraude. Dit omdat dat het probleem vooral zit in de strafrechtelijke keten en de benadering van identiteitsfraude.
De Kunst, M.J.J. en prof J.J.M. van Dijk, *Slachtofferschap van fraude. Een explorerend onderzoek naar de impact diverse vormen van financieel-economische criminaliteit* (Tilburg 2009).	Het stuk gaat over de definitie en de vormen van 'Fraude'. Identiteitsfraude wordt in dit stuk als een van de vele varianten van fraude omschreven. In de paragraaf over identiteitsfraude staan drie casussen beschreven waar sprake is geweest van identiteitsfraude. De wereld van het slachtoffer wordt aan het einde van de paragraaf die ingaat op wel mooi samengevat.
Nationale Ombudsman. *Herzien openbaar rapport, rapportnummer 2009/199* (september 2009).	Dit rapport handelt over de casus Kowsoleea. Door de zeer uitgebreide casus wordt de schade die slachtoffers kunnen lopen in allerlei facetten behandeld. Ron Kowsoleea wordt al sinds 1994 gedupeerd door identiteitsfraude. In allerlei informatiesystemen van verschillende bestuursorganen staat ten onrechte strafrechtelijke informatie over hem vermeld. De zaak Kowsoleea heeft veel stof doen opwaaien in de Kamer en was mede de aanleiding om het Centraal Meldpunt Identiteitsfraude en –fouten op te richten, zie kopje 'Kafka en kafkaësk: De gevolgen van een gedigitaliseerde samenleving'.
De Vries, U.R.M.Th. e.a. e.d., *Identiteitsfraude: een afbakening, een internationale begripsvergelijking en analyse van nationale strafbepalingen* (Den Haag 2007).	Interessant in dit onderzoek is de zoektocht naar de definitie van identiteitsfraude en hoe men er internationaal connotatie aan geeft. Er worden wel een aantal interessante invalshoeken gekozen als het gaat hoe we naar slachtofferschap kunnen kijken. Met name de begrippen 'horizontale en verticale identiteitsfraude' krijgen veel aandacht in het onderzoek. . In veel gevallen is er namelijk sprake van meerdere slachtoffers en is het niet een natuurlijk persoon, maar de overheid of een private partij die gedupeerd is.
Expertgroep Shopping 2020, *Veiligheid en Fraude* (Ede januari 2014).	Dit rapport is samengesteld door een expertgroep bestaande uit veiligheids- en fraude experts en internetwinkel expert. Het rapport geeft inzicht wat voor (identiteits)fraude internetwinkels tegenkomen en hoe ze deze kunnen bestrijden, dan wel voorkomen. Ze geven een aantal goede en interessante tips aan winkeliers over awereness, risico's van elektronische identiteit en verzekeringen die je als winkel kunt afsluiten tegen de gevolgen van (identiteitsfraude).
Govcert.nl, Nationaal Trendrapport Cybercrime en Digitale Veiligheid (Den Haag oktober 2010).	Het rapport gaat over cybercrime in algemene zin en laat zien hoe kwetsbaar de overheid is voor de gevolgen hiervan, ook richting burger. De burger is nauwelijks op de hoogte van de gevaren die kunnen ontstaan als gevolg van identiteitsfraude. Financiële instellingen vergoeden tot nu toe namelijk vaak de schade van burger;

	als gevolg van cybercriminaliteit, zoals skimming, identiteitsdiefstal bij online bankieren en misbruik van creditcards. Deze aanpak leidt ertoe dat burgers zelf bij genoemde deze soorten fraude nauwelijks economische schade ondervinden. Kortom: er is sprake van afwenteling van het risico? Zolang de financiële instellingen vergoeden, leidt de burger geen schade. De vraag is alleen hoe lang dat systeem zo blijft werken.
Minister van Binnenlandse Zaken en Koninkrijksrelaties dr. R.H.A. Plasterk, 'Kamerbrief over integrale visie op de aanpak van identiteitsfraude'(Den Haag 20 december 2013) kenm. 2013-0000776428.	Dit document bestaat eigenlijk uit twee losse onderdelen. Het betreft een brief én een bijlage waarin de overheid zijn visie geeft op het bestrijden, en de preventie, van identiteitsfraude. De monitor identiteit in cijfers van Panteia is tegelijk met de brief aan de Tweede Kamer aangeboden. De grote ontwikkeling op het gebied van identiteitsfraude is dat fraudeurs grensoverschrijdend werken en vaak tot een grote criminele organisaties behoren. De aanpak gaat ook in op de mogelijke gevolgen voor slachtoffers en wat de burger van de overheid mag verwachten op het gebied van preventie, bestrijding, verantwoordelijkheid en aansprakelijkheid. En hoe de overheid beter kan en moet samenwerken.
Panteia, *Identiteit in cijfers.* In opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (15 december 2014 tweede editie).	Het rapport is een monitor op de ontwikkeling van identiteitsfraude. Hoe ziet ons identificatiestelsel eruit, hoe identificeren we ons en hoe vaak komt fraude of fouten voor? De doelstelling van deze monitor is het in kaart brengen van gegevens over het identiteitsstelsel, de praktijk van identificatie en identiteitsfraude. Hoofdstuk 4 is geheel gewijd aan identiteitsfraude. Ze geven hierin aan wat er mogelijk is als het gaat om identiteitsfraude en wat de omvang van de praktijk is, op basis van cijfers van diverse instituties zoals de Koninklijke Marechaussee, RDW en IND.
PWC, *Omvang van identiteitsfraude & maatschappelijke schade in Nederland* (Amsterdam 2012).	Dit rapport is een eerste aanzet om de omvang van identiteitsfraude en alle praktijken hierbinnen in kaart te brengen. Het is een kwantitatief onderzoek dat zich richt op de hoeveelheid identiteitsfraude gevallen en de schade daar van. In hoofdstuk 4 en 5 wordt behandeld hoe groot de omvang is van identiteitsfraude in respectievelijk de private en de publieke sector.
PWC, *Centraal Meld- en informatiepunt Identiteitsfraude. Analyse meldingen 2011-2012* (Amsterdam april 2013).	Het bevat de analyse van de meldingen van het CMI. De kerngegevens van de meldingen komen aan bod, de behandeling van de meldingen door het CMI, de kwalitatieve trends en inzichten uit andere rapportages. Alles tezamen moet een indicatie geven over de aard en omvang van identiteitsfraude in Nederland. Ze geven tevens een inzicht in de geschatte schade die slachtoffers lijden. Opmerkelijk feit is dat het aantal aangiften bij de politie ieder jaar daalt.
PWC, *2013-update onderzoek 'Omvang van identiteitsfraude & maatschappelijke schade in Nederland* Amsterdam mei 2013).	Het meeste recente stuk als het gaat om cijfers over identiteitsfraude (mei 2013). De basis van het onderzoek is een enquête onder burgers, de respons was 5039. De onderzoekers geven aan dat deze update vooral een indicatief beeld moet scheppen. Opvallend is dat 84 procent van de slachtoffers zich meldt bij de politie, en dat slechts een 25% bekend IS met het Centraal Meld- en informatiepunt Identiteitsfraude en –fouten.
Speerstra, T., en Henstra, L. 'Identiteitsonderzoek in de strafrechtsketen' in: *Het Tijdschrift voor de Politie*, 2014, nr4.	Het artikel gaat in op het feit dat de overheid nog geen hoogwaardige identificatiehuishouding heeft, en dat er daardoor regelmatig fouten worden gemaakt bij registratie van personen. Bovendien is frauderen binnen het huidige systeem vrij eenvoudig. Het stuk gaat ook in op de fouten die op verschillende plekken in de keten

	worden gemaakt, zoals bij de politie. Het gevolg van die versnippering van systemen en gehanteerde identificatie processen is dat het slachtoffer gegevens lastig kan herstellen. De overheid zou de verantwoordelijkheid voor systeembeheer dan ook serieuzer moeten nemen. Door de sterke verzuiling in het strafrechtslandschap, is een structurele, over de eigen organisatie-grenzen heen werkende samenwerking nodig, maar vooralsnog opereert iedere organisatie op zijn eigen eilandje. Verder gaat het artikel kort in op de 'praktische houding van onverschilligheid' bij de politie, als het gaat om identiteitsfraude.
Paulissen, L., en Van Wilsem, J. , *Dat heeft iemand anders gedaan: een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland (Politie & wetenschap (82), 2015)*	In deze studie wordt identiteitsfraude onderzocht als (internationaal) fenomeen. Met name relevant voor dit onderzoek zijn de resultaten van een peiling onder een representatief panel, waarbij incidentie en omvang van de schade van identiteitsfraude is bepaald. Het gaat om antwoorden van een tweejaarlijkse peiling en de resultaten zijn gebaseerd op de antwoorden uit 2010 en 2012.

Bijlage C. Bevraagde organisaties

Organisatie	Geïnterviewde perso(o)n(en)
Hulpverlenende organisaties en meldpunten	
Centraal Meldpunt Identiteitsfraude en –fouten (CMI)	Mevrouw H. van der Sluys (coördinator CMI) en mevrouw N. Kneijber (medewerker CMI)
Fraudehelpdesk	Mevrouw F. van Eck (managing director)
College bescherming persoonsgegevens (CBP)	Mevrouw S. Artz (senior inspecteur)
Nationale Ombudsman	De heer M. Ramlal (beleidsadviseur) en mevrouw M. Bannier (senior onderzoeker)
Slachtofferhulp Nederland	De heer V. Jammers (lid raad van bestuur)
Landelijk Meldpunt Internetoplichting (LMIO, onderdeel van de nationale politie)	De heer G. van der Linden (projectleider LMIO) en de heer E. Coenen (analist)
Overheidsorganisaties waar de fraude gepleegd wordt	
Rijsoverheid en uitvoeringsorganisaties	
Rijksdienst voor Wegverkeer (RDW)	De heer W. Leutscher (Adviseur Expertisecentrum rijbewijzen) en de heer K. Zweegman (klachten coördinator en adviseur, voorzitter voertuigketen)
Logius	De heer R. Derksen (senior analist / adviseur fraudebestrijding) en de heer M. Claessen (strategie en financiën)
Expertisecentrum Vreemdelingen, Identificatie en Mensenhandel (EVIM, nationale politie)	De heer A. van der Meijden (senior adviseur identiteitmanagement) en de heer G.J. Lucas (senior adviseur identiteitmanagement)
Openbaar Ministerie	De heer T. Voskuil (landelijk coördinator bestrijding horizontale fraude)
Expertisecentrum Identiteitsfraude en Documenten (ECID, samenwerking tussen KMAR en nationale politie)	De heer R. Koster (leidinggevende ECID), de heer M. van Gaalen (unit manager bestrijding identiteitsfraude) en de heer R. Brabander (Operationeel specialist B)
Belastingdienst	De heer A. van Lohuizen (teamleider) en de heer M. Zijlstra (jurist)
UWV	De heer R. de Waal (senior beleidsadviseur), mevrouw S. Koole (business analist divisie Klant en Service), de heer N. Djuricic (risico-onderzoeker directie handhaving) en de heer B. Pootjes (klantcommunicatie adviseur directie Klant en Service)
SVB	De heer M. Wissink (senior medewerker sectie bijzonder onderzoek)
DUO	Mevrouw A. Luth, (afdeling handhaving en inspectie)
Kamer van Koophandel (KvK)	Mevrouw W. te Lintelo (beleidsadviseur handelsregister)
Immigratie en Naturalisatiedienst (IND)	De heer PJ. Louw (manager koppelingsbureau & kwaliteitsbewaking) en de heer J. Welfing (adviseur handhaving)
Financial Intelligence Unit (onderdeel van de nationale politie)	Anoniem

Gemeenten	
Gemeente Amsterdam (Team Identiteitsfraude, TIF)	De heer D. Rutgers (manager meldingen & handhaving) en de heer M. Wachter (teamleider en coördinator)
Gemeente Den Haag	De heer R. de Jonge (teammanager BRP en burgerlijke stand)
Gemeente Rotterdam	Mevrouw L. van der Ploeg (senior projectmanager Expertise Burgerzaken)
Gemeente Maastricht	De heer H. Hendrix (accountmanager reizen en documenten)
Gemeente Enschede	De heer H. Balke (senior projectmedewerker)
Gemeente Groningen	De heer A. Brands (beleidsmedewerker) en de heer H. Woldring (Adviseur Planning en Bedrijfsvoering)
Gemeente Hulst	De heer M. Marin (hoofd Publiekszaken)
Gemeente Hilvarenbeek	De heer R. van Gils (beleidsmedewerker Burgerzaken)
Gemeente Helmond	De heer B. Brinks (team manager integrale ondersteuning) en de heer H. Maes (teamleider stadswinkel)
Private organisaties	
E-commerce	
Thuiswinkel.org	Mevrouw E. Oldhoff (beleidsadviseur en jurist)
Coolblue	De heer A.A. van Dijk (manager security) en mevrouw K. Bijl (teamleider debiteuren)
Wehkamp	De heer N. Pinto (teamleider Fraude Lacent/Wehkamp Finance)
Scheer & Foppen	De heer Korlaar (financieel manager)
Blokker	De heer Haverkamp (fraude en dervingcoördinator)
Mediamarkt	De heer Meijt (directeur veiligheid)
Telecom	
Ziggo	De heer J. van 't Schip (medewerker risk en control en integriteitsmanagement)
KPN	De heer J. Kasper (Manager Telecomfraude)
Websend (moederbedrijf Studentmobiel en GSM-wijzer)	De heer T. Borsboom (directeur/eigenaar)
Banken	
NVB	Mevrouw Muriel Kok (adviseur veiligheidszaken)
Rabobank	De heer R. Bleijs (adviseur fraude, detectie en identiteit)
SNS Reaal (moedermaatschappij van o.a. ASN-bank)	Mevrouw I. Lammerts (adviseur veiligheidszaken)
KNAB	De heer J. (Fraude Coördinator & Security)

Zorgverzekeraars	
Kenniscentrum Fraudebeheersing (Zorgverzekeraars Nederland)	Het kenniscentrum heeft de vragen voorgelegd aan haar leden (vandaar een anonieme respons)
De Friesland Zorgverzekeraar	Anoniem
CZ	Anoniem
Zilveren Kruis/Achmea	Anoniem
Zorg en Zekerheid	Anoniem
Leveranciers	
PostNL	De heer A. Verkaik (directeur security)
Overige personen/organisaties	
Koninklijke Notariële Beroepsorganisatie	Mevrouw C. Heck
Mevrouw M. Genova (journalist, auteur van o.a. “Komt een vrouw bij de hacker”)	Mevrouw M. Genova

Bijlage D. Resultaten juridische verkenning

In deze bijlage vindt u de uitwerking van de onderzoeksvragen van de juridische verkenning. De opzet van de verkenning en de algemene conclusies vindt u in Hoofdstuk 7.

Inleiding

In de onderliggende verkenning wordt gekeken naar de juridische mogelijkheden van herstel en compensatie wanneer de burger zich tot de overheid wendt met de mededeling dat hij slachtoffer is geworden van identiteitsfraude. Om in aanmerking te komen voor vergoeding van schade door een overheidsinstelling, moet de betrokkenheid van die instelling bij de fraude worden vastgesteld. Zonder enige vorm van betrokkenheid is een verplichting tot vergoeding van schade vanuit het huidige juridische kader moeilijk denkbaar. In hoofdstuk 7 zijn daarom drie 'situaties' onderscheiden waarin de betrokkenheid van de overheid kan worden onderzocht op de mogelijkheden van herstel en/of compensatie. Het gaat hierbij respectievelijk om (1) de overheid als *beslissingsbevoegde* bij materieel benadelende besluiten, (2) om de overheid als *verantwoordelijke voor basisregistraties* en de bij haar geregistreerde gegevens en (3) om de overheid als *aangesproken partij* ter vergoeding van anderszins geleden schade. Situaties 1 en 2 zien op het herstel van de (directe) gevolgen van identiteitsfraude, situatie 3 ziet op een eventuele aansprakelijkheid voor overige schade na identiteitsfraude. In de hiernavolgende paragrafen komen de drie situaties terug en worden zij vergeleken met gelijksoortige situaties in procedures tussen civiele partijen. Omdat naar ons idee het slachtoffer eerst de gevolgen van de identiteitsfraude ongedaan gemaakt wenst te zien, voordat het aan de eventuele schadeaspecten toekomt, wordt in de paragrafen A1 tot en met A3 eerst het hersteltraject besproken, waarna in paragrafen B1 en B2 de (civielrechtelijke) aansprakelijkstelling wordt behandeld. Elke paragraaf sluit af met een tussenconclusie. De eindconclusie is opgenomen in Hoofdstuk 7.

A1. Ongedaan maken gevolgen identiteitsfraude; bestuursrecht

In het eerste deel van deze verkenning wordt allereerst stilgestaan bij de bestuursrechtelijke kant van identiteitsfraude, waarbij met name de jurisprudentie over terugvorderingsbesluiten interessant is. Wanneer individuele besluiten (beschikkingen) zijn aangevraagd (al dan niet via DigiD) met gebruikmaking van de gegevens van een ander (bijvoorbeeld aanvragen om bijstand of toeslagen), kan later blijken dat de toekenning van de gelden onterecht bleek te zijn. Het betrokken 'bestuursorgaan' besluit dan vaak tot terugvordering van de gelden bij degene op wiens naam de aanvraag staat. Slachtoffers van identiteitsfraude hebben de gelden echter nooit ontvangen en gaan tegen het terugvorderingsbesluit in bezwaar en beroep. In de bestuursrechtelijke jurisprudentie staat vervolgens de vraag centraal: *hoe dient een bestuursorgaan om te gaan met een beroep op identiteitsfraude bij terugvorderingen van uitgekeerde, maar beweerdelijk nooit ontvangen, gelden?* Voordat deze vraag wordt onderzocht is het eerst van belang kort stil te zijn bij de context van de besluitvorming door het bestuursorgaan. Aan een terugvordering gaat immers een eerder (positief) besluit vooraf. Van dat besluit is het slachtoffer vaak niet op de hoogte. In hoeverre dient een bestuursorgaan zich ervan te vergewissen dat de bij haar binnengekomen aanvragen correct zijn?

(On)juiste gegevens in de aanvraag

Als uitgangspunt voor alle door bestuursorganen genomen besluiten geldt dat deze besluiten op een zorgvuldige wijze tot stand moeten zijn gekomen. Dat is neergelegd in artikel 3:2 van de Algemene wet bestuursrecht (Awb): "Bij de voorbereiding van een besluit vergaart het bestuursorgaan de nodige kennis omtrent de relevante feiten en de af te wegen belangen." Die relevante feiten beperken zich niet alleen tot gegevens benodigd voor het nemen van het materiële besluit, maar omvatten ook informatie over de wijze waarop de aanvraag is ingediend (voldoet de aanvraag aan de gestelde vormvereisten?) en informatie over de persoon van de aanvrager (is deze persoon gerechtigd de aanvraag in te dienen?).

In de situatie dat een slachtoffer van identiteitsfraude wordt geconfronteerd met een terugvordering van nooit ontvangen gelden, is het eerdere, aan de terugvordering ten grondslag liggende, besluit reeds genomen op basis van onjuiste gegevens. De feitelijke aanvrager is bijvoorbeeld niet de persoon wiens gegevens in de aanvraag staan vermeld, terwijl het bankrekeningnummer wel tot de feitelijke (frauderende) aanvrager behoort. Het zorgvuldigheidsbeginsel van artikel 3:2 Awb gaat niet zo ver dat het bestuursorgaan onrechtmatig handelt als het dergelijke ongerijmdheden niet opspoort. Zo hoeft een aanvraag – behoudens bijzondere wettelijke voorschriften – niet steeds vergezeld te gaan van een kopie van een legitimatiebewijs en hoeft een bestuursorgaan niet te controleren wie de houder is van het door de aanvrager opgegeven rekeningnummer. Het is primair aan de aanvrager om zorg te dragen voor juiste gegevens in de aanvraag. Dat voorkomt onnodige formalisering, bespoedigt het besluitvormingsproces en vergroot de dienstbaarheid van het betrokken bestuursorgaan. Bij schriftelijke aanvragen kan bovendien worden vermoed dat een handtekening onder een aanvraag afkomstig is van de persoon die met zijn persoonsgegevens op de aanvraag staat vermeld. Een bestuursorgaan mag dus in beginsel vertrouwen op de juistheid van de handtekening, alsook op de juistheid van de verder door de aanvrager aangeleverde gegevens.

Alleen wanneer evident sprake is van valse bescheiden en gegevens (zoals een kopie van een zichtbaar vervalst identiteitsbewijs of gegevens die overduidelijk afwijken van gegevens die bij het bestuursorgaan bekend zijn) bestaat er reden voor het bestuur nadere inlichtingen van de aanvrager te verlangen, alvorens het besluit op aanvraag te nemen. Doet het dat niet, dan kunnen de gevolgen van het besluit voor diens rekening komen.

Elektronische aanvragen

Sinds de inwerkingtreding van de Wet elektronisch bestuurlijk verkeer in 2004 maakt de Awb het mogelijk een aanvraag elektronisch in te dienen en te ondertekenen. De Awb stelt aan de elektronische *handtekening* de eis dat de "methode die daarbij voor authentificatie wordt gebruikt voldoende betrouwbaar is, gelet op de aard en de inhoud van het elektronische bericht" (artikel 2:16 Awb, met verwijzing naar artikel 3:15a BW). Onder een elektronische handtekening wordt verstaan een handtekening die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie (artikel 3:15a lid 4 BW). Afhankelijk van de gebruikte methode kunnen, zo blijkt uit artikel 3:15a BW, verschillende gradaties bestaan in (het vermoeden van) betrouwbaarheid van een elektronische handtekening ter controle van de authenticiteit van het bericht en de identiteit van de

ondertekenaar. Afhankelijk van de gebruikte techniek kan er in dat kader sprake zijn van een 'gewone' elektronische handtekening, een *geavanceerde* elektronische handtekening (artikel 3:15a lid 3 BW) of een *gekwalificeerde* elektronische handtekening (artikel 3:15a lid 2 BW).

Uit de onderzochte jurisprudentie komt naar voren dat besluiten genomen op grond van vermeende identiteitsfraude niet zelden elektronisch via een overheidswebsite zijn ingediend. Om toegang te krijgen tot de desbetreffende overheidswebsite of het betreffende elektronische aanvraagformulier dient de aanvrager veelal in te loggen met zijn of haar DigiD-gegevens. In sommige gevallen dient de verzending van de aanvraag nogmaals te worden bevestigend met een DigiD-autorisatie. Gelet op de inrichting van de DigiD-autorisatie kwalificeert de ondertekening met DigiD zich niet als een *gekwalificeerde* of een *geavanceerde* handtekening. In de rechtswetenschap bestaat bovendien twijfel of DigiD als inlog- of ondertekeningsmethode in alle gevallen voldoet aan de eisen die gesteld worden aan het begrip 'elektronische handtekening' uit artikel 2:16 Awb jo. 3:15a lid 4 BW. Slechts wanneer de DigiD-'ondertekening' daadwerkelijk gegevens vasthecht of logisch associeert met (andere) gegevens uit het bericht is sprake van een (gewone) elektronische handtekening.[35] Door de koppeling van de handtekening met deze andere gegevens wordt het vermoeden gesterkt dat de gegevens uit de aanvraag afkomstig zijn van de werkelijke persoon van de aanvrager. De mate waarin het bestuursorgaan mag uitgaan van de gegevens uit de aanvraag, wordt dus mede bepaald aan de hand van het 'betrouwbaarheidsniveau' van het systeem waarmee de elektronische handtekening is geplaatst, al blijkt de Afdeling bestuursrechtspraak van de Raad van State (ABRvS) geen hoge eisen te stellen aan de onderzoeksplicht van bestuursorganen zodra gebruik wordt gemaakt van een autorisatie via DigiD. Deze hoge eisen gelden evenmin als er in het geheel geen sprake is van een 'elektronische handtekening', maar slechts van een DigiD-inlogprocedure.[36]

Uit de uitspraak van 24 april 2013 (*JB* 2013/125) volgt dat gebruikmaking van DigiD-autorisatie in beginsel een voldoende betrouwbare methode voor het indienen (en/of ondertekenen) van een aanvraag is, zodat het in beginsel voor moet worden gehouden dat een aanvraag op naam van betrokkene ook daadwerkelijk door hem is ingediend. Dit is alleen anders als er duidelijke indicaties bestaan dat de genoemde methode ten tijde van de aanvraag onvoldoende betrouwbaar was.

Betrokkene werd in deze zaak geconfronteerd met een terugvordering van ruim 50.000 euro aan onterecht ontvangen kinderopvangtoeslag. Betrokkene had steeds aangegeven de aanvragen kinderopvangtoeslag niet te hebben ingediend en de gelden ook niet te hebben ontvangen (de bij de aanvraag opgegeven bankrekening stond op naam van een hem onbekende BV). De

[35] A.M. Klingenberg, 'De handtekening in het elektronisch bestuurlijk verkeer', *JBPlus* 2011, p. 129-137 (i.h.b. p. 135); J. Vlug, 'DigiD: goed geregeld? Het verschijnsel DigiD rechtsstatelijk bekeken, *Digitale publicatiereeks Recht en Overheid (Academie voor Wetgeving)* 2012.

[36] Zo volgt immers uit de hierna te bespreken uitspraak van 24 april 2013. De Afdeling baseert haar oordeel in deze uitspraak weliswaar (mede) op artikel 2:16 Awb, maar merkt daarbij ook op dat niet te achterhalen viel op wiens DigiD de litigieuze aanvragen waren ingediend. In dat geval is er dus geen sprake geweest van een aanhechting of logische associatie van andere gegevens met de ondertekening en is artikel 2:16 Awb strikt genomen niet van toepassing op de aanvraag. (ABRvS 24 april 2013, *JB* 2013/125, rov. 5.1-5.3).

Afdeling komt tot de conclusie dat tijdens de zitting is komen vast te staan dat de omgeving van DigiD voor een bepaalde periode kwetsbaar is geweest en niet valt uit te sluiten dat de aanvraag door een ander is ingediend. Bovendien bleken er meer gevallen bekend te zijn waarbij de toeslag op het rekeningnummer van de bewuste BV werd gestort, terwijl de aanvraag op naam van een ander stond. De Belastingdienst mocht om die reden de reeds uitbetaalde voorschotten niet terugvorderen van betrokkene. In haar noot onder deze uitspraak accentueert Overkleeft-Verburg het feit dat het in eerdere procedures niet was gelukt de betrouwbaarheid van DigiD in twijfel te trekken. Slechts als betrokkene met bewijzen kan komen dat DigiD in de bewuste periode niet voldoende betrouwbaar is geweest, bestaat ruimte voor het betwisten van de ingediende aanvraag om kinderopvangtoeslag (en daarmee voor de betwisting van de terugvordering).

In de hier aangehaalde uitspraak mocht de Belastingdienst dus niet vertrouwen op de bij haar ingediende *aanvraag*, waardoor de terugvordering automatisch van tafel ging. Net als bij schriftelijke aanvragen gaat de onderzoeksplicht van het bestuursorgaan bij elektronische aanvragen niet zo ver dat het moet controleren of de identiteit van de aanvrager klopt. Pas wanneer het slachtoffer van identiteitsfraude met voldoende bewijzen aannemelijk kan maken dat het de aanvraag niet zelf heeft ingediend, bestaat ruimte de initiële aanvraag te vernietigen. Vaak zal dat echter niet lukken, zeker niet wanneer de aanvraag is ingediend met een (vervalste) fysieke handtekening, waarbij immers in het geheel geen autorisatiesystemen aan te pas komen. Dat neemt echter niet weg dat ook in die gevallen terugvordering onrechtmatig kan zijn.

Het ongedaan maken van de gevolgen van identiteitsfraude door de bestuursrechter

Om zicht te krijgen in de wijze waarop de bestuursrechter om gaat met een beroep op identiteitsfraude in een procedure tegen een materieel benadelend besluit (zoals een terugvordering), worden hieronder enkele uitspraken van de Centrale Raad van Beroep (sociale zekerheidsgeschillen) en de Afdeling bestuursrechtspraak van de Raad van State (overige geschillen) besproken.

De Centrale Raad van Beroep (CRvB) gaat er van uit dat een intrekking en terugvordering van een eerder toegekend recht op bijstand een belastend besluit is, waardoor het aan het bestuursorgaan is om de nodige kennis te vergaren over de relevante feiten en omstandigheden en op het bestuursorgaan de bewijslast rust ten aanzien van de vraag of is voldaan aan de voorwaarden om tot intrekking van het recht op bijstand over te gaan.[37] In de zaken waarover de Centrale Raad oordeelde ging het om te veel ontvangen inkomsten doordat uitkeringsgerechtigden bepaalde inkomsten uit arbeid zouden hebben verzwegen. Uit vaste jurisprudentie van de Raad blijkt dat intrekking van bijstand alleen kan worden gebaseerd op gegevens van de Belastingdienst als deze gegevens door het UWV of door de werkgever worden bevestigd:

> ‘In gevallen waarin appellant van de Belastingdienst informatie ontvangt over door een belanghebbende genoten inkomsten uit arbeid, heeft appellant naar vaste rechtspraak in voldoende mate aan de onder 4.1 bedoelde onderzoeksplicht en bewijslast voldaan, indien de uit het onderzoek naar dat signaal van de werkgever en/of

[37] CRvB 12 mei 2009, JB 2009/153, ECLI:NL:CRVB:2009:BI4343.

het Uitvoeringsinstituut werknemersverzekeringen (Uwv) verkregen gegevens de informatie van de Belastingdienst bevestigen. Daarbij is wel vereist dat de uit beide bronnen verkregen gegevens op relevante onderdelen, waaronder het sofinummer van de belanghebbende, de werkgever, de arbeidsverhouding en het loon van de belanghebbende met elkaar overeenstemmen. Indien het gaat om werkzaamheden op basis van een uitzendovereenkomst, ligt het naar het oordeel van de Raad uit een oogpunt van een evenwichtige bewijslastverdeling en gelet op de aan appellant als bestuursorgaan ter beschikking staande onderzoeksmogelijkheden tevens op de weg van appellant om in het kader van het onderzoek naar een belastingsignaal bij het uitzendbureau naast de loongegevens ook de naam van de inlener(s) op te vragen.' (CRvB 12 mei 2009, rov. 4.2).

Als deze gegevens overeenkomen dan is het aan belanghebbende om de onjuistheid van die gegevens aannemelijk te maken (rov. 4.3).[38]
Hier vindt dus een 'check' plaats met andere registers. Van belang hierbij is echter de recente herstructurering van de basisregistraties, zoals de Basisregistratie adressen en gebouwen (BAG), de Basisregistratie personen (BRP) of de Basisregistratie Inkomen (BRI). Sinds deze herstructurering geldt voor verschillende basisregistraties een gebruiksplicht voor bestuursorganen bij het vervullen van hun publiekrechtelijke taak. Dit houdt in dat zij zogenaamde 'authentieke gegevens' niet alleen bij hun uitvoerings- en handhavingstaken dienen te gebruiken, maar ook dat zij in beginsel van de juistheid van die gegevens dienen uit te gaan. Bestuursorganen mogen dus niet meer zelf gegevens inwinnen bij bedrijven of burgers, waardoor hun administratieve lasten verminderd worden. Overkleeft-Verburg heeft hierover opgemerkt dat de juistheid van de informatie in de basisregistraties een rechtsvermoeden wordt, wat is terug te zien in de bewijswaarde van basisregistraties in latere jurisprudentie. Dit kan het aannemelijk maken van onjuistheden voor de burger frustreren. Immers, hoe centraler de gegevens geregeld worden, des te moeilijker is de controle ervan en des te groter is het gevolg van identiteitsfraude.[39] Het principe van eenmalige gegevensopslag en multifunctioneel gebruik zorgt er volgens Overkleeft-Verburg ook voor dat de burger in een andere verhouding tot het bestuursorgaan komt te staan. Niet langer dient alleen geprocedeerd te worden over het materieel benadelende besluit, maar ook over eventuele weigeringen om de registraties aan te passen (zie daarover onder A3). Nu de basisregistraties vaak worden beheerd door andere bestuursorganen, dienen meerdere overheidsinstellingen bij het oplossen van het probleem te worden betrokken. Het bestuursorgaan dat het materieel benadelende besluit neemt, kan zich bovendien gemakkelijk tegen het beroep van het slachtoffer verweren door te wijzen op de gebruiksplicht en het slachtoffer door te sturen naar het registerverantwoordelijke bestuursorgaan. Dat dit niet louter theorie is, blijkt ook uit de jurisprudentie.

In het geschil dat ten grondslag lag aan de uitspraak van de rechtbank Amsterdam van 24 september 2013 (ECLI:NL:RBAMS:2013:6141) ging het om spookbewoning in een studentenhuis door een vermogende derde. In de procedure tegen het terugvorderingsbesluit van de beweerdelijk te veel ontvangen huurtoeslagen stelde de Belastingdienst zich op het standpunt dat het mocht uitgaan van de

[38] Zie ook CRvB 11 mei 2010, ECLI:NL:CRVB:2010:BM4996, rov. 4.5.

[39] Zie G. Overkleeft-Verburg, 'Basisregistraties en rechtsbescherming. Over de dualisering van de bestuursrechtelijke rechtsbetrekking', *NTB* 2009, p. 70 e.v., zie ook de – zeer uitvoerige – noot van Overkleeft-Verburg over de gebruiksplicht onder CRvB 14 september 2012, JB 2012/213.

gegevens uit het (toen nog) GBA en het geen eigen onderzoek naar de juistheid ervan mocht verrichten. Voor herstel van de onjuiste gegevens verwees de Belastingdienst appellant naar de gemeente als verantwoordelijk orgaan voor de registratie. Omdat partijen ook over een eerdere toeslagjaar hadden geprocedeerd, herhaalde de rechtbank allereerst de hoofdlijnen uit de eerdere uitspraak van de Afdeling bestuursrechtspraak:

> "2.1 De Afdeling bestuursrechtspraak van de Raad van State (hierna: de Afdeling) heeft in een eerdere zaak tussen partijen in haar uitspraak van 18 januari 2012 (te vinden op www.rechtspraak.nl, onder European Case Law Identifier ECLI:NL:RVS:2012:BV1205) een oordeel gegeven over de herziening en terugvordering van aan eiser verstrekte huurtoeslag over het toeslagjaar 2007: (...) voorop staat dat de gegevens in de basisadministratie betrouwbaar en duidelijk moeten zijn alsmede dat de gebruikers van de gegevens erop moeten kunnen vertrouwen dat de gegevens in beginsel juist zijn. De Afdeling heeft daarbij verder overwogen dat voor het wijzigen van eenmaal in de basisadministratie geregistreerde gegevens of het plaatsen van een aantekening van onjuistheid bij bepaalde gegevens, gelet op het systeem van de Wet GBA, onomstotelijk zal moeten vaststaan dat deze feitelijk onjuist zijn [*zie ook hierna onder A3, MT/MV*]. Hieruit volgt voor de onderhavige zaak dat de Belastingdienst van de inschrijving van [betrokkene] op het adres van [naam] mocht uitgaan, nu daarbij geen aantekening van onjuistheid was geplaatst. Het lag voorts op de weg van [naam] om zich tot de gemeente als beheerder van de basisadministratie te wenden met het verzoek de vermelding van [betrokkene] op zijn woonadres ongedaan te maken in welk verband verklaringen van getuigen een rol kunnen spelen. Dat heeft hij, zoals hij ter zitting heeft erkend, niet gedaan. Hij heeft voorts zijn stelling dat het voor hem niet mogelijk was langs die weg de adresgegevens van [betrokkene] te laten wijzigen dan wel daarbij een aantekening van onjuistheid te laten plaatsen, niet aannemelijk gemaakt. Onder deze omstandigheden heeft de Belastingdienst uit de vermelding van [betrokkene] in de GBA op het woonadres van[naam] mogen afleiden dat deze medebewoner was. De omstandigheid dat een belanghebbende die het niet eens is met een besluit van het ene bestuursorgaan, in dit geval de Belastingdienst, zich tot een ander bestuursorgaan, in dit geval het college van burgemeester en wethouders, moet wenden om tot een oplossing van zijn geschil te komen, is de consequentie van het werken met een basisadministratie, waarbij uitsluitend de beheerder van die administratie wijzigingen kan doorvoeren."

Nadat de procederende student zich daarna wel tot het college van burgemeester en wethouders had gewend, achtte de rechtbank de gebruiksplicht van de Belastingdienst niet meer absoluut:

> 2.2 In de huidige zaak – die betrekking heeft op het toeslagjaar 2008 – zijn de omstandigheden echter wat anders komen te liggen dan zij in de hiervoorgenoemde Afdelings-uitspraak lagen. (...) De Afdeling overweegt in de eerdere tussen partijen gegeven uitspraak dat gebruikers er op moeten kunnen vertrouwen dat de GBA-gegevens in beginsel juist zijn. (...) Verder overweegt de Afdeling in die uitspraak dat het op de weg van [naam] lag om zich tot de gemeente als beheerder van de basisadministratie te wenden met het verzoek de vermelding van [betrokkene] op zijn woonadres ongedaan te maken. Dat heeft eiser inmiddels gedaan. De rechtbank acht gezien het hiervoor onder 2.3, 2.4 en 2.5 overwogene meer dan aannemelijk gemaakt, dat [betrokkene] ondanks zijn GBA-inschrijving niet feitelijk op het adres woonde. De rechtbank is dan ook van oordeel dat verweerder onder genoemde omstandigheden uit GBA-inschrijving van [betrokkene] niet heeft mogen afleiden dat hij feitelijk een medebewoner was.

Uit de jurisprudentie blijkt dus dat het mogelijk is om benadelende besluiten van tafel te krijgen als betrokkene bij het bestuursorgaan *voldoende aannemelijk* kan maken dat hij slachtoffer is geworden van identiteitsfraude. Dit geldt volgens de rechtbank Amsterdam ook voor besluiten die zijn gebaseerd op onjuiste gegevens in basisregistraties.

Hoe moet een betrokkene nu aannemelijk maken dat de gegevens onjuist zijn? De uitspraak van het CRvB van 11 mei 2010, (ECLI:NL:CRVB:2010:BM4996) geeft hiervan een voorbeeld:

> in deze uitspraak betrof het een fout in de gegevensadministratie tussen verschillende partijen (de bank, de Belastingdienst en de gemeente). De sociale dienst beweerde dat appellant over twee bankrekeningen beschikte waarvan hij ten onrechte geen melding had gemaakt. De bank weigerde aanvankelijk met een beroep op het bankgeheim om aan appellant duidelijk te maken op wiens naam de rekeningen stonden. Appellant meldde de sociale dienst dat de bank de medewerking weigerde en dat hij zonder hulp van de sociale dienst niet verder zou komen. Ook deed hij bij de politie aangifte van identiteitsfraude. Deze actieve inspanningen van appellant hadden voor de sociale dienst aanleiding moeten zijn om nader onderzoek te doen op basis van artikel 3:2 Awb. Dit onderzoek was ten onrechte achterwege gelaten. Ook was ten onrechte van gemeentewege elke hulp aan betrokkene geweigerd, onder verwijzing naar een beweerdelijk op hem rustende inlichtingenverplichting of bewijslast. Van eigen schuld van betrokkene kon onder deze omstandigheden niet worden gesproken.

Het actief inspannen als slachtoffer om identiteitsfraude terstond aan te kaarten en proberen ongedaan te maken blijkt essentieel om met succes een beroep op identiteitsfraude te kunnen doen.[40]

Duidelijk niet voldoende is bijvoorbeeld de enkele aangifte van identiteitsfraude, zoals blijkt uit CRvB 29 oktober 2013 (ECLI:NL:CRVB:2013:2334, rov. 4.3). Het betrof hier het verzoek om terug te komen op een eerder genomen terugvorderingsbesluit. Appellant had pas twee jaar nadat het terugvorderingsbesluit was genomen aangifte van identiteitsfraude gedaan bij de politie. Hoewel het CRvB dit tijdsverloop niet expliciet in de motivering noemt, maakt het CRvB wel duidelijk dat het enkele feit dat appellant aangifte heeft gedaan onvoldoende is om het bestuursorgaan te verplichten van het terugvorderingsbesluit terug te komen.

Hoewel de precieze grenzen ten aanzien van de vereiste inspanningen door slachtoffers van identiteitsfraude niet scherp uit de jurisprudentie kunnen worden gedestilleerd, is wel duidelijk dat het slachtoffer oplettend dient te zijn en adequaat dient te reageren op signalen die op onjuistheden wijzen. Dit legt een verantwoordelijkheid op de burger om brieven afkomstig van overheidsinstellingen nauwgezet te lezen en te controleren op onjuistheden, bij gebreke waarvan een later beroep op identiteitsfraude kan worden bemoeilijkt. Mede om die reden slaagde het beroep op fraude niet ten aanzien van een terugvorderingsbesluit van voorschotten kinderopvangtoeslag. De toeslag was via de DigiD van appellante aangevraagd onder vermelding van het juiste

[40] Vergelijk ABRvS 12 februari 2014, ECLI:NL:RVS:2014:396, rov. 4.2 en ARBvS 8 juli 2015, ECLI:NL:RVS:2015:2121, rov. 5.2).

postadres (en het juiste bankrekeningnummer) van appellante. Omdat de Belastingdienst brieven naar dat adres had gestuurd en de gelden op het opgegeven bankrekeningnummer had overgemaakt, had appellante op de hoogte kunnen zijn dat zij kinderopvangtoeslag ontving. Het betoog dat een hulpverlener de gegevens zonder toestemming van appellante had gebruikt, slaagde niet.[41]

Tussenconclusie: in beginsel mogen bestuursorganen vertrouwen op de juistheid van (persoons)gegevens in de bij hen binnengekomen aanvragen. Voor het voldoen aan de zorgvuldigheidsplicht bij de besluitvorming hebben basisregistraties bovendien een hoge bewijswaarde. Het is aan de burger om aannemelijk te maken dat de bij het bestuursorgaan bekende gegevens onjuist zijn. Dat aannemelijk maken zal in de regel alleen slagen als het slachtoffer alert en proactief heeft gehandeld vanaf het moment dat de fraude hem bekend kon zijn.

A2. Ongedaan maken gevolgen identiteitsfraude; civiel recht

In de civielrechtelijke jurisprudentie gaat het over verbintenissen die zijn aangegaan zonder dat de betrokkene in kwestie daar zelf mee heeft ingestemd. Te denken valt aan het afsluiten van telefoonabonnementen op naam van een ander, het digitaal aankopen van producten met betaling achteraf, of het gebruik van bankpassen van een ander. Belangrijk in de jurisprudentie is de vraag hoe de verkopende partij de identiteitscontrole heeft uitgevoerd. Anders dan in het bestuursrecht maken civiele partijen minder gebruik van (centrale) registers en vallen zij niet onder een gebruiksplicht. Met name de vergelijking tussen aanvragen met DigiD en online aankopen is daarom interessant.

In de civielrechtelijke jurisprudentie staat de vraag centraal: *hoe dient een verkopende partij om te gaan met een beroep op identiteitsfraude na verzoek om nakoming van een verbintenis?* De algemene lijn die uit de civiele jurisprudentie volgt is dat degene die zich op de rechtsgevolgen van een overeenkomst beroept, de stelplicht en de bewijslast draagt van het feit dat die overeenkomst ook daadwerkelijk tot stand is gekomen tussen de verkoper en de gedaagde partij. Bij gemotiveerde betwisting van de zijde van gedaagde, rust op de verkoper dus de bewijslast van het tot stand komen van een rechtsgeldige overeenkomst.

Stelplicht en bewijslast

Een voorbeeld dat laat zien hoe de bewijslast in het civiele recht is verdeeld, biedt een vonnis van de rechtbank Limburg.[42] In naam van gedaagde was op 16 oktober 2013 bij de website ‘Pleinshoppen’ een bestelling gedaan voor twee stofzuigers. Deze waren afgeleverd op een adres waar appellant ooit korte tijd woonde. Het bedrijf dat namens Pleinshoppen de nakoming van de digitale koopovereenkomst vorderde, Direct Pay, stelde dat appellant gehouden was de koopovereenkomst na te komen en ook de buitengerechtelijke incassokosten te voldoen. Gedaagde betwistte dat hij een geldige koopovereenkomst was aangegaan dan wel dat iemand bevoegd was om dit in zijn naam te doen. De vraag was derhalve of tussen Pleinshoppen en gedaagde een koopovereenkomst

[41] ABRvS 3 juni 2015, ECLI:NL:RVS:2015:1739, rov. 2.1.

[42] Rechtbank Limburg 17 september 2014, ECLI:NL:RBLIM:2014:8004.

tot stand was gekomen op grond waarvan gedaagde gehouden was tot betaling.
De rechter constateerde dat op Direct Pay de stelplicht, en bij gemotiveerde betwisting de bewijslast rust van de stelling dat een geldige koopovereenkomst tot stand was gekomen. Direct Pay had in de visie van de rechtbank niet aan deze stelplicht voldaan door na te laten nader te onderbouwen dat een overeenkomst tot stand was gekomen. Immers het was niet komen vast te staan dat de verklaring om de koopovereenkomst aan te gaan van gedaagde afkomstig was. Het lag in dat kader op de weg van Direct Pay om de identiteit aan te tonen van degene die het aanbod van Pleinshoppen heeft aanvaard en daarmee de contract sluitende partij was geworden. De rechtbank aanvaardde niet het door Direct Pay ingenomen standpunt dat het risico van de onduidelijkheid omtrent de identiteit van de contract sluitende partij voor risico van de gedaagde komt.
Deze invulling van de bewijslast wordt bevestigd door een andere zaak, waarin creditcardmaatschappij ICS beweerde dat een geldige creditcardovereenkomst tot stand was gekomen tussen haar en gedaagde en op basis daarvan gedaagde wenste te veroordelen tot betaling van 7652,06 euro aan openstaande facturen. De kantonrechter stelde vast dat ICS zich beriep op de rechtsgevolgen van de door haar gestelde overeenkomst. Daarmee droeg zij tevens de stelplicht en de bewijslast van het bestaan van die overeenkomst. Gedaagde betwistte dat een overeenkomst tot stand was gekomen en stelde dat zij slachtoffer was geworden van identiteitsfraude. Zij ontving in 2009, toen de bestellingen op haar naam werden gedaan, thuishulp en was toen beweerdelijk niet tot werkzaamheden in staat. ICS kon slechts aanvoeren dat de bestedingen in en rond Naarden zijn gedaan en dat gedaagde niet had blijk gegeven van een frauduleus bestedingspatroon. ICS had de creditcard verstuurd naar aanleiding van een telefoongesprek maar had niet concreet gemaakt welke gegevens bij die aanvraag waren verstrekt. Evenmin had ICS die gegevens en de aanvraag geverifieerd aan de hand van een recente handtekening van gedaagde. Dat gedaagde daarvan geen aangifte had gedaan, was niet beslissend. ICS was er niet in geslaagd te bewijzen dat er, ten einde de creditcard te activeren, was gebeld vanaf een op naam van gedaagde geregistreerd telefoonnummer. Eiser had kennelijk niet gecontroleerd dat de koper daadwerkelijk gedaagde was, zodat de totstandkoming van de koopovereenkomst tussen eiser en gedaagde niet voldoende is komen vast te staan.

Bovenvermelde uitspraken geven blijk van een voor de verkopende partij strenge lijn. De bewijslast dat degene op wiens naam de bestelling is gedaan ook een geldige koopovereenkomst heeft *willen* sluiten, rust op degene die stelt dat deze overeenkomst tot stand is gekomen. Voor internetverkoopbedrijven kan het in dit verband van belang zijn om te werken met een unieke inlogcode, die de koper via zijn e-mail ontvangt. Ook een elektronische handtekening kan de gebruiker helpen om de identiteit vast te stellen (vergelijk de eisen van artikel 3:15a BW uit de vorige paragraaf). In elk geval vereist de rechtbank in deze zaak uitdrukkelijke controlewerkzaamheden om succesvol te kunnen betogen dat een overeenkomst tot stand was gekomen.

Rol van eigen schuld

Het leerstuk van de eigen schuld speelt echter eveneens een rol bij zaken over misbruik van gegevens. Een voorbeeld is een geschil over een online aangevraagde lening met een BizKey.[43] De BizKey is een

[43] Rechtbank Rotterdam 20 april 2011, ECLI:NL:RBROT:2011:BQ7167.

apparaat waarmee met een zelfgekozen vijfcijferige code kan worden ingelogd op Bizner's toepassing voor online bankieren. Eenmaal ingelogd kan de klant in een beveiligde omgeving geld overboeken of leningen afsluiten. De gedaagde partij was volgens de rechter onvoldoende zorgvuldig omgegaan met de BizKey. Degene die bij Bizner een lening had aangegaan bleek een voormalig werknemer van gedaagde, die tevens huisgenoot was van gedaagde en in die hoedanigheid een computer met gedaagde deelde, waarop zij gezamenlijk een rekening beheerden en zo ook beiden toegang hadden tot de BizKey en de code. Gedaagde beweerde dat Bizner haar zorgplicht had geschonden omdat zij ten aanzien van de lening niet of nauwelijks had geverifieerd of gedaagde degene was die deze lening had aangevraagd. De rechtbank oordeelde echter dat gebleken was dat de leningen alleen met behulp van de aan de identiteit van [gedaagde] gekoppelde BizKey konden worden aangevraagd, zodat op Bizner niet een extra verplichting rustte om de identiteit van de aanvrager (nogmaals) vast te stellen. Kortom: indien het misbruik is te wijten aan gebrek aan zorg van gedaagde, dan wordt dat in beginsel aan hem toegerekend, tenzij gedaagde omstandigheden stelt en bewijst die een zodanig gebrek aan zorg uitsluiten (vgl. HR 19 november 1993, *NJ* 1994, 622).

Coulance

In Gerechtshof Arnhem-Leeuwarden 4 november 2014 (ECLI:NL:GHARL:2014:8585) is een voorbeeld te zien van 'coulance'. Op naam van het slachtoffer van identiteitsfraude zijn diverse telefoonabonnementen afgesloten. Het slachtoffer heeft hiervan aangifte gedaan en heeft de fraude direct bij de betrokken partijen (waaronder KPN, The Phone House en Telfort) gemeld. KPN bericht het slachtoffer uiteindelijk dat zij de vordering op het slachtoffer niet zal overdragen aan een incassobureau, maar deze als een verlies zal nemen. Wel wordt het slachtoffer geregistreerd bij Preventel, zodat betrokkene de komende jaren niet een nieuw telefoonabonnement kan afsluiten. Vraag bij het Gerechtshof is of deze registratie terecht is. Gelet op de accuratesse van betrokkene wordt de registratie onjuist bevonden.

Tussenconclusie: als gegevens onvoldoende veilig worden opgeborgen, speelt de eigen schuld een belangrijke rol in civiele geschillen. Wel moet de eisende partij bij gemotiveerde betwisting door gedaagde zich ervan hebben vergewist dat de consument daadwerkelijk de identiteit heeft waarvoor hij zich uitgeeft. Op dit punt wijkt het uitgangspunt in het civiele recht af van dat in het bestuursrecht. Waar bestuursorganen in beginsel geen onderzoek hoeven te doen naar de juistheid van handtekeningen of de werkelijke identiteit achter de naam en gegevens van de aanvrager, lijkt het civiele recht meer eisen te stellen aan de identiteitscontrole. Gelijk aan het bestuursrecht helpt een elektronische handtekening (zoals een BizKey; vergelijk DigiD) de wederpartij evenwel om aan deze controle te voldoen.

A3: Aanpassen onjuiste gegevens in (basis)registratie

Zodra een materieel besluit genomen wordt op grond waarvan de geadresseerde constateert dat hij het slachtoffer is geworden van identiteitsfraude, ligt het op de weg van het slachtoffer om zo snel mogelijk aan de bel te trekken bij het desbetreffende bestuursorgaan, een bezwaar- of beroepsprocedure te starten en aannemelijk te maken dat de gegevens waarop het bestuursorgaan zich heeft gebaseerd onjuist zijn.

Hierboven is al opgemerkt dat het slachtoffer een bestuursorgaan tegen zich kan zien die gebruik heeft gemaakt van gegevens die zijn opgenomen in een basisregistratie. Met de herstructurering van deze registraties en de daarbij ingevoegde gebruiksplicht, komt het niet zelden voor dat het benadelende besluit voor het slachtoffer haar oorsprong vindt in een onjuist gegeven in een basisregistratie. Zo blijkt het bijvoorbeeld in de praktijk relatief gemakkelijk voor een persoon om zich in te schrijven op het adres van een ander, zonder diens medeweten. Een vervalsing van een huurcontract met handtekening en een kopie van een identiteitsbewijs kan de opname in het BPR bewerkstelligen. Als deze spookbewoner vervolgens meer inkomen verdient dan de oorspronkelijke bewoner, kan deze laatste geconfronteerd worden met stopzetting en terugvordering van bijvoorbeeld bijstand of huurtoeslag. Het is dan aan het slachtoffer om náást een procedure ter herstel van het benadelende besluit ook een correctieprocedure te starten van gegevens in de basisregistratie. Hiervoor dient veelal contact te worden gezocht met een ander bestuursorgaan.

EVRM als minimumwaarborg

Het EVRM speelt bij de ongedaanmaking van onjuiste gegevens in (basis)registraties een belangrijke minimumwaarborg voor het slachtoffer. Zoals hierna zal blijken beschermt het EVRM ook de identiteits- en persoonlijke gegevens van de burger. Zodra een toekomstige inbreuk op de bescherming van deze gegevens mogelijk is of blijft, wordt het beschermingsregime van het EVRM 'geactiveerd'. Het EVRM is daarom niet zozeer van belang bij de ongedaanmaking van de materiële benadelende besluiten, zoals deze onder paragraaf A1 centraal stonden, maar wel bij de ongedaanmaking van onjuiste gegevens in registraties die de basis kunnen vormen voor toekomstige besluiten en handelingen. Dit blijkt duidelijk uit de zaak-*Romet*, waarbij het laten voortbestaan van onjuiste registraties in het kentekenregister de kans op identiteitsfraude vergroot. Alvorens op deze specifieke zaak in te gaan, wordt eerst een algemene schets gegeven van het beschermingsbereik van het EVRM.

Het EVRM verlangt in beginsel onthouding van de overheid tot het maken van een inbreuk op, bijvoorbeeld, de vrijheid van meningsuiting of het recht op privacy. Toch verlangt het EVRM soms ook actief optreden van de overheid, die positieve maatregelen moet nemen om te voorkomen dat identiteitsfraude wordt gepleegd of dat burgers met de negatieve gevolgen daarvan blijven zitten (de leer van de zgn. 'positieve verplichtingen').
Voor identiteitsfraude is vooral artikel 8 van het EVRM van belang, dat het respect voor het privé- en het familieleven regelt. Lidstaten bij het Verdrag dienen zich te onthouden van interventie in het recht op respect voor het privéleven van de burger. Artikel 8 EVRM legt de Staat dus vooreerst een negatieve, onthoudings-, verplichting op. Slechts wanneer een wettelijk voorschrift in beperking in dit recht voorziet, de uitoefening van deze beperking noodzakelijk is in een democratische samenleving én de beperking een legitiem doel dient, is het de overheid toegestaan inbreuk te maken op het privéleven. Hier valt onder meer te denken aan opsporingsmethoden in het kader van een strafrechtelijk onderzoek.

Het Europese Hof voor de Rechten van de Mens legt het recht op respect voor het privéleven ruim uit. In onder andere het arrest

Reklos & Davourlis t. Griekenland[44] heeft het EHRM het recht op respect voor het privéleven nader geduid. Gegevens, zoals in casu een foto, die betrekking hebben op de unieke karakteristieken van een persoon en die het mogelijk maken de betreffende persoon te onderscheiden van anderen, vallen volgens het Hof onder de reikwijdte van artikel 8 EVRM. Ook de identiteit van een persoon en daarmee gepaard gaande diens persoonsgegevens vallen onder het mensenrecht.

Bovenal heeft het EHRM aangenomen dat de leer van de 'positieve verplichtingen' ook opgeld doet in het kader van artikel 8 EVRM. De Staat dient zich in beginsel niet alleen te onthouden van inmenging in het privéleven van het individu, maar dient onder omstandigheden ook actief maatregelen te treffen om te voorkomen dat het recht op respect voor het privéleven door anderen kan worden geschaad. De plicht om actief maatregelen te nemen om een inbreuk door anderen te voorkomen is goed zichtbaar in de *Romet*-zaak.[45] In deze zaak speelde identiteitsfraude een centrale rol.

Klager, de heer Romet, verliest in september 1995 zijn rijbewijs en verkrijgt pas anderhalf jaar later (vanwege de aan de aanvraag van een nieuw rijbewijs verbonden kosten), in maart 1997, een nieuw rijbewijs. In de tussenliggende periode heeft de Rijksdienst voor het Wegverkeer 1737 voertuigen op zijn naam geregistreerd in het Kentekenregister. Als gevolg daarvan kreeg klager een groot aantal aanslagen motorrijtuigenbelasting en werd hij regelmatig beboet wegens overtreding van de Wet Mulder (Wet administratiefrechtelijke handhaving verkeersvoorschriften). Klager werd enige tijd gegijzeld vanwege het niet betalen van de boeten; ook werd zijn uitkering stopgezet aangezien het vermoeden bestond dat zijn vermogen voldoende was gelet op het hoge aantal op zijn naam geregistreerde auto's. Pogingen om de Rijksdienst voor het wegverkeer de op zijn naam staande registraties te laten corrigeren, lopen op niets uit. Weliswaar annuleerde de RWD in 2004 nog enige resterende registraties, maar deed dat niet met terugwerkende kracht omdat dit de betrouwbaarheid van het systeem zou ondermijnen (zie ook hierna). De Algemeen Directeur van de Rijksdienst Wegverkeer had afwijzend beslist op de door Romet op grond van artikel 40 lid 2 Kentekenreglement gedane verzoeken om 1497 kentekenregistraties van voertuigen op zijn naam met terugwerkende kracht vervallen te verklaren. Hij baseerde zich daarbij op een uitspraak van de Afdeling bestuursrechtspraak Raad van State dat de rechtszekerheid zich verzet tegen het met terugwerkende kracht schrappen van kentekens, omdat dit de integriteit van het kentekenregister zou aantasten (ABRvS 4 februari 2004, ECLI:NL:RVS:2004:AO2879). De nationale procedures tegen de weigering die Romet tegen de weigering door de RWD aanspande liepen op niets uit (ABRvS 7 december 2005, *JB* 2006/50 m.nt. van Overkleeft-Verburg).

Het EHRM oordeelt dat de Nederlandse staat een inbreuk heeft gepleegd op artikel 8 EVRM door na te laten het rijbewijs zo spoedig mogelijk na de aangifte van vermissing ongeldig te verklaren. Hierbij was het volgens het Hof niet relevant of de klager zelf voldoende actie heeft ondernomen tegen de valse registraties. Het Hof stelt in dat verband vast dat direct na de ongeldig verklaring van het gestolen

[44] EHRM 15 januari 2009, *EHRC* 2009/34.

[45] EHRM 14 februari 2012, *AB* 2012/275, m.nt. Barkhuysen en Van Emmerik, *EHRC* 2012/87.

rijbewijs, in maart 1997, de ongeldige registraties op naam van klager ophielden en dit dus liet zien dat het handelen van de staat directe invloed had op de inbreuk op artikel 8 EVRM.

Mede naar aanleiding van deze zaak hebben verschillende auteurs de Nederlandse Staat opgeroepen meer werk te maken van de erkenning van de positie van slachtoffers van identiteitsfraude en dat zij hun juridische mogelijkheden om dat te doen, zoals het correctierecht, ook in de praktijk dienen toe te passen, en waar nodig organisatorische maatregelen moeten nemen om weerstand bij organisaties tegen aanpassing van registraties weg te nemen.[46] Barkhuysen en Van Emmerik stellen voorts dat ook Nederlandse rechters en het bestuur (de Afdeling bestuursrechtspraak Raad van State en de RWD) te weinig oog hebben gehad voor de gevolgen voor klager van de onverkorte toepassing van de onderhavige regelgeving.

De essentie van de uit *Romet* volgende rechtsregel is later nog aan bod gekomen in een uitspraak van de Rechtbank Midden-Nederland van 9 augustus 2013 (ECLI:NL:RBMNE:2013:3268, rov. 10):

> "In tegenstelling tot wat eiser heeft aangevoerd, volgt uit de zaak van Romet tegen Nederland niet een algemene verplichting voor verweerster om in het geval waarin zij kennis heeft van een onjuiste tenaamstelling in het Kentekenregister, tot correctie hiervan over te gaan, maar volgt uit deze zaak dat verweerster hiertoe verplicht is wanneer een schending van artikel 8 van het EVRM op de loer ligt omdat de betrokkene – door geen actie te ondernemen – aan mogelijke identiteitsfraude wordt blootgesteld. In deze zaak was eiser onderwerp van een strafrechtelijk onderzoek en zijn de auto's in dat kader door het Openbaar Ministerie in beslag genomen. In zoverre is de zaak van eiser niet vergelijkbaar met de zaak van Romet tegen Nederland. Omdat de auto's zich in eisers geval onder het Openbaar Ministerie bevonden, lag het gevaar van identiteitsfraude hier niet op de loer."

Uit de *Romet*-zaak blijkt aldus dat de overheid actief dient op te treden als het door eigen toedoen *de kans op misbruik van identiteitsgegevens* kan voorkomen. Op het moment dat een slachtoffer zich bij de overheidsinstelling meldt en duidelijk is dat hij het slachtoffer is geworden van identiteitsfraude, dient het onverwijld maatregelen te treffen om verder misbruik te voorkomen. Een vervolgvraag is dan *hoe en in welke mate* het slachtoffer de identiteitsfraude duidelijk moet maken.

Nationale jurisprudentie

Hoewel overheidsorganen op basis van het EVRM dienen over te gaan tot onverwijlde aanpassing van gegevens indien een verder misbruik van identiteitsgegevens op de loer ligt, dient het slachtoffer wel duidelijk te maken dat er daadwerkelijk sprake is van identiteitsfraude. De Nederlandse jurisprudentie laat zien dat de bewijslast daarvoor geheel bij het slachtoffer ligt en de aannemelijkheid van de fraude alleen nog niet voldoende is.

Voor het herstellen van fouten in de GBA gelden volgens vaste jurisprudentie strenge eisen rondom de zekerheid dat de huidige registratie een fout bevat:

> "Zoals de Afdeling eerder heeft overwogen (...) dient voorop te worden gesteld dat de gegevens in de gba betrouwbaar en duidelijk

[46] B.J. Koops en N. S. van der Meulen stellen, 'Van preventie naar risicoacceptatie en herstel voor slachtoffers in Nederlands beleid tegen identiteitsfraude', *NJB*, 2012/1414, afl. 25, p. 1706.

> moeten zijn. De gebruikers van de gegevens moeten erop kunnen vertrouwen dat de gegevens in beginsel juist zijn. Voor het wijzigen van eenmaal in de gba geregistreerde gegevens zal gelet op het systeem van de Wet gba onomstotelijk moeten vaststaan dat deze feitelijk onjuist zijn."[47]

De burger heeft dus de bewijslast aan te tonen dat de gegevens feitelijk onjuist zijn. Dat bewijs moet 'onomstotelijk' zijn. De uitspraak van 2 mei 2009 van de ABRvS (*JB* 2009/114) geeft hiervan een voorbeeld. Appellante beriep zich erop dat ene heer X zonder medeweten van haar op haar adres stond ingeschreven. Dit had direct gevolgen voor haar huurtoeslag. Omdat heer X bij inschrijving in de gba een brief wist te overhandigen met de schriftelijke toestemming met handtekening van appellante en een kopie van haar identiteitsbewijs, slaagde appellante er niet in om te bewijzen dat de heer X niet daadwerkelijk op haar adres woonachtig was.

Voor de bewijslast van de burger maakt het daarom een groot verschil of het *aannemelijk* moet maken dat de gegevens waarop een bestuursorgaan zich moet baseren onjuist zijn (zoals te zien is in jurisprudentie onder A1), dan wel dat hij moet *bewijzen* dat de in het register opgenomen gegevens niet kloppen. Uit de rechtspraak blijkt daarom ook dat procedures tegen benadelende besluiten sneller kans van slagen hebben, dan aanpassingsprocedures van basisregistraties.

Als het de betrokkene vervolgens lukt om te bewijzen dat de gegevens onjuist zijn, is het echter nog niet altijd mogelijk om de gegevens ook *met terugwerkende kracht* gewijzigd te krijgen.

[47] ABRvS 21 januari 2015, ECLI:NL:RVS:2015:134 rov. 2.1.

In rechtspraak onder de oude GBA oordeelde de Afdeling bestuursrechtspraak van de Raad van State bijvoorbeeld dat "noch artikel 82 van de Wet GBA, noch enige andere wettelijke bepaling het college de bevoegdheid geeft om de datum van een adreswijziging te baseren op de dag waarop de betrokkene feitelijk op een nieuw adres is gaan wonen."[48] Aanpassing met terugwerkende kracht werd dus niet mogelijk geacht. Ook ten aanzien van het kentekenregister is het *niet* verlenen van terugwerkende kracht hoofdregel:

> "Volgens vaste jurisprudentie van de Afdeling (onder meer uitspraak van 13 juni 2012 in zaak nr. 201106493/1/A3), kan niet worden geoordeeld dat het door de RDW gevoerde beleid om in beginsel geen terugwerkende kracht te verlenen aan besluiten, inhoudende ongeldigverklaring van het kentekenbewijs van een voertuig, niet redelijk is. De zuiverheid van het kentekenregister en de rechtszekerheid van de tenaamstelling van voertuigen rechtvaardigen een dergelijk beleid. De RDW verleent slechts bij hoge uitzondering terugwerkende kracht aan een besluit inhoudende de ongeldigverklaring van het kentekenbewijs van een voertuig. Dit beleid is thans neergelegd in artikel 40c, tweede en derde lid, van het Kr."[49]

Voor het aannemen van deze 'hoge uitzondering', is wel vereist dat het slachtoffer – vergelijk onder A1 – oplettend, adequaat en actief handelt zodra de onjuistheid hem bekend kon zijn:

> "De RDW heeft ter zitting verklaard dat door hem jaarlijks enkele malen wordt gecontroleerd of voor in het kentekenregister

[48] ABRvS 16 oktober 2013, ECLI:NL:RVS:2013:1567.

[49] ABRvS 8 juli 2015, ECLI:NL:RVS:2015:2121.

> opgenomen motorvoertuigen een geldige verzekering is afgesloten, en dat, wanneer wordt vastgesteld dat een motorvoertuig als onverzekerd staat geregistreerd, de betrokkene daarover bij brief wordt bericht. De RDW heeft voorts, door [appellante] onweersproken, ter zitting desgevraagd verklaard dat [appellante] ook in de periode tussen de aangifte van de diefstal en de brief van 2011, door de RDW op vorenbedoelde wijze op de hoogte is gebracht van het onverzekerd zijn van het voertuig. De Afdeling is van oordeel dat het op de weg van [appellante] lag om, zodra zij de bedoelde informatie van de RDW ontving, te bewerkstelligen dat door de politie een gestolensignaal zou worden geplaatst, zoals uiteindelijk in 2011 is gebeurd. Dat zij dit heeft nagelaten, dient voor haar rekening en risico te komen. Gelet op het vorenstaande heeft de rechtbank terecht overwogen dat geen bijzondere omstandigheden aan de orde zijn die de RDW ertoe hadden moeten nopen van het door hem gevoerde beleid af te wijken."[50]

Tussenconclusie: vanuit het EVRM-recht rust op de Staat een positieve verplichting om bij onjuiste registratie van gegevens maatregelen te treffen als identiteitsfraude op de loer ligt. Het is daarbij evenwel aan het slachtoffer om duidelijk te maken dat er sprake is van fraude. In dat kader staat volgens vaste jurisprudentie voorop dat de in de basisregistratie opgenomen gegevens betrouwbaar en duidelijk moeten zijn en dat de gebruiker van de registratie moet kunnen vertrouwen op de juistheid ervan. Dat vertaalt zich in de bewijslast voor het slachtoffer. Anders dan bij het ongedaan maken van materieel benadelende besluiten kan niet meer worden volstaan met aannemelijkheid, maar moet de onjuistheid onomstotelijk vaststaan.

[50] ABRvS 12 februari 2014, ECLI:NL:RVS:2014:396.

Herziening met terugwerkende kracht is daarom alleen bij hoge uitzondering mogelijk.

A4. Het vergoeden van schade in het hersteltraject

De voorgaande paragrafen hadden betrekking op het herstel van de directe gevolgen van de identiteitsfraude: materiële benadelende besluiten van de overheid die vernietigd werden en vermeende privaatrechtelijke verbintenissen die het slachtoffer niet konden worden tegengeworpen. Afhankelijk van de omstandigheden van het geval is het denkbaar dat het slachtoffer ook andere schade lijdt. In hoeverre deze schade voor vergoeding in aanmerking komt, wordt hierna in onderdeel B besproken. In ieder geval kan één schadepost reeds hier worden vermeld en dat zijn de proceskosten. Zowel in het bestuursprocesrecht als in het burgerlijke procesrecht is uitgangspunt dat de in het gelijk gestelde partij een *gedeelte* van de door haar gemaakte proceskosten vergoed krijgt van de wederpartij.[51] Dit is een wettelijk stelsel met forfaitaire tarieven. Het slachtoffer ontvangt dus veelal een vergoeding die lager is dan de daadwerkelijk gemaakte kosten. Van andere vergoedingen in het hersteltraject is ons in de jurisprudentie niet gebleken.

B1. Civielrechtelijke aansprakelijkheid voor identiteitsfraude

Ten aanzien van een mogelijke civiele aansprakelijkheid van de overheid (die speelt in alle gevallen waarin de schade niet wordt veroorzaakt door appellabele besluiten) dient zich een aantal vragen aan.

[51] In het bestuursrecht geldt dit overigens alleen in de verhouding 'overheid aan burger'. Procederende burgers kunnen, behoudens misbruiksituaties, niet worden veroordeeld in de proceskosten van het bestuursorgaan.

1. Kan de overheid op basis van specifieke wettelijke voorschriften aansprakelijk worden gehouden als een burger slachtoffer wordt van identiteitsfraude?
2. Zo nee, kan de overheid dan op basis van een actie uit onrechtmatige daad (artikel 6:162 BW) aansprakelijk worden gehouden als een burger slachtoffer wordt van identiteitsfraude?

In de paragrafen hieronder worden beide vragen nader onderzocht.

Een specifieke wettelijke basis voor aansprakelijkstelling

Bij de mogelijkheden om de overheid aansprakelijk te stellen, is het van belang eerst te bezien of er een (specifieke) wettelijke basis is die in een procedure voorziet ter vergoeding van schade door identiteitsfraude. De enige – voor zover wij kunnen overzien – wettelijke basis is artikel 49 Wet bescherming persoonsgegevens (Wbp). Dit artikel luidt als volgt:

1. *Indien iemand schade lijdt doordat ten opzichte van hem in strijd wordt gehandeld met de bij of krachtens deze wet gegeven voorschriften zijn de volgende leden van toepassing, onverminderd de aanspraken op grond van andere wettelijke regels.*
2. *Voor nadeel dat niet in vermogensschade bestaat, heeft de benadeelde recht op een naar billijkheid vast te stellen schadevergoeding.*
3. *De verantwoordelijke is aansprakelijk voor de schade of het nadeel, voortvloeiende uit het niet-nakomen van de in het eerste lid bedoelde voorschriften. De bewerker is aansprakelijk voor die schade of dat nadeel, voor zover ontstaan door zijn werkzaamheid.*
4. *De verantwoordelijke of de bewerker kan geheel of gedeeltelijk worden ontheven van deze aansprakelijkheid, indien hij bewijst dat de schade hem niet kan worden toegerekend.*

Dit artikel zou als grondslag voor de toekenning van schadevergoeding kunnen dienen wanneer degene die verantwoordelijk is voor de verwerking van persoonsgegevens (en dat kan zowel een natuurlijke persoon, een rechtspersoon of een bestuursorgaan zijn) nalaat om te voldoen aan verschillende verplichtingen die de Wbp hen oplegt. Zo verlangt artikel 11 lid 2 Wbp dat de verantwoordelijke de nodige maatregelen treft opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, 'juist en nauwkeurig zijn'. Hier is het de vraag of, en zo ja, wanneer de gegevens als gevolg van ID-fraude niet juist blijken te zijn, de verantwoordelijke daar niet beter op had moeten letten. Deze verantwoordelijkheid kan een rol spelen bij de toekenning van administratieve identiteiten door de overheid bij het inschrijven in de basisregistratie(s) en bij het vaststellen van de identiteit wanneer een persoon met de identiteit van een ander een transactie overeenkomt met een leverancier (zowel bij overheid als bedrijf). Ook artikel 13 Wbp is in dit kader van belang; dit artikel verlangt dat de verantwoordelijken voor de verwerking van persoonsgegevens de in dit artikel neergelegde 'passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking'.

Welke maatregelen in dit verband precies kunnen worden verlangd, komt hierna nog aan de orde. Voor nu is van belang te constateren dat het niet naleven van de in artikel 11 of artikel 13 Wbp genoemde

zorgplicht om te zorgen voor een veilige verwerking van persoonsgegevens tot een vergoedingsplicht kan leiden van de verantwoordelijken voor die dataverwerking. Daarbij stelt artikel 13 wel de voorwaarde dat er causaliteit bestaat tussen het nalaten en de schade (lid 3) en dat de schade hem kan worden toegerekend (lid 4).

Artikel 11 speelt voornamelijk een rol in situaties waarin gegevens door de verantwoordelijke verkeerd in het systeem zijn geplaatst. Hierbij kan gedacht worden aan typefouten en verkeerde, al dan niet automatische, koppelingen. De zorgplicht van artikel 11, tweede lid Wbp strekt echter niet zo ver dat de verantwoordelijke voor de gegevensopslag ook moet instaan voor de juistheid van de informatie zoals die door de betrokkene is aangeleverd. Artikel 13 Wbp speelt in de jurisprudentie vooral een rol bij (digitale) gegevensuitwisseling tussen artsen/geneeskundige hulpverleners en patiënten t.a.v. medische gegevens. Jurisprudentie waarin de zorgplicht uit artikel 13 Wbp relevant wordt geacht bij een schadevergoedingsactie op basis van artikel 49 Wbp hebben wij echter niet gevonden. Een van de vragen die daarbij speelt is welke betekenis toekomt aan de frase uit lid 2 dat het 'nadeel dat niet in vermogensschade bestaat naar billijkheid wordt vergoed'. De Memorie van Toelichting bij dit artikel geeft daarover (25 892, nr. 3) geen aanwijzingen. Vermeldenswaard is wel dat een vergelijkbare bepaling stond in de (niet langer geldende) Wet persoonsregistraties. Naar aanleiding van vragen van de CDA-fractie antwoordde de regering destijds dat:

> "bij de omgang met persoonsgegevens nadeel vaak niet in geld valt uit te drukken. Met de toelichting is bedoeld te zeggen dat vergoeding van ideële, dus immateriële schade op haar plaats is omdat vaak van vermogensschade, dus materiële schade geen sprake is. Onder materiële schade wordt verstaan nadeel dat in geld valt uit te drukken. Daarom schrijft artikel 9, tweede lid, ook voor dat de hoogte van de schadevergoeding naar billijkheid wordt vastgesteld. Dit zou niet nodig zijn indien de schade wel in geld zou zijn uit te drukken".[52]

Destijds werd ook de vraag gesteld, door leden van de fractie van de VVD, of artikel 9, tweede lid, naast artikel 6.1.9.11 van het Nieuwe Burgerlijke Wetboek (thans art. 6:106 BW) nog noodzakelijk is. Zo ja, dan zou naar hun oordeel toch meer aansluiting bij dat artikel moeten worden gezocht. Naar aanleiding hiervan antwoordde de regering dat, hoewel artikel 9, tweede lid, na invoering van Boek 6 wellicht kan vervallen, voor handhaving zou pleiten dat "iedere twijfel omtrent de mogelijkheid van immateriële schadevergoeding daardoor wordt uitgesloten"[53].

De invoering per 1 januari 2016 van de Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp (*Stb*. 2015, 230) regelt een meldplicht voor datalekken in de Wbp. De meldplicht is afgekeken van de meldplicht uit artikel 11.3a Telecommunicatiewet. Dit artikel beoogt de persoonsgegevens en de persoonlijke levenssfeer van de abonnee of gebruiker van een aanbieder van een elektronische communicatiedienst beter te beschermen tegen inbreuken op de veiligheid van persoonsgegevens en de ongunstige gevolgen die dit kan hebben voor de persoonlijke levenssfeer van degene wiens persoonsgegevens het betreft.

[52] *Kamerstukken II* 1986-87, 19 095, nr. 6, p. 49 (Memorie van Antwoord Wet persoonsregistraties).

[53] Idem.

Aansprakelijkstelling en de algemene actie uit onrechtmatige daad
In situaties waarin een bijzondere wettelijke aansprakelijkstelling geen soelaas biedt, zou een actie uit onrechtmatige daad een juridische mogelijkheid kunnen bieden tot vergoeding van geleden schade na identiteitsfraude. Voordat aansprakelijkheid uit onrechtmatige daad kan worden aangenomen, dienen eerst *ten minste* een drietal vragen te worden beantwoord. Uit het hiernavolgende blijkt dat het antwoord op deze vragen in het kader van identiteitsfraude niet altijd gemakkelijk is te geven en een aansprakelijkstelling niet zelden in de weg zullen staan. Achtereenvolgens komt aan bod, de vraag:

a. Waaruit bestaat de onrechtmatige daad en kan deze onrechtmatige daad aan de overheid worden toegerekend?
b. Wat is de schade?
c. Bestaat er een causaal verband tussen de onrechtmatige daad en de schade?

Ad a. Onrechtmatige daad/toerekening

Onrechtmatige appellabele besluiten
Ten aanzien van de onrechtmatigheid van het handelen van de overheid moet een onderscheid worden gemaakt tussen twee situaties: ten eerste die waarin sprake is van een appellabel *besluit* dat door de bestuursrechter wordt vernietigd en ten tweede de situatie dat de overheid op andere wijze onrechtmatig handelt. Bij de eerste situatie valt te denken aan een besluit tot terugvordering van bijstand bij een persoon op wiens naam bijstand is aangevraagd, maar die de bijstand nooit heeft ontvangen. Als het besluit tot terugvordering vernietigd wordt door de bestuursrechter of het bestuursorgaan dit besluit op materiële gronden herroept, dan moet dat besluit worden aangemerkt als een onrechtmatige daad, wat eveneens een grondslag biedt voor de toekenning van schadevergoeding. Veel rechtspraak over schade ten gevolge van onrechtmatige besluiten in de context van identiteitsfraude is er niet. Wel valt te wijzen op CRvB 11 mei 2010, ECLI:NL:CRVB:2010:BM4996.

> Hierin ging het om een terugvorderingsbesluit dat werd genomen toen het bestuursorgaan vermoedde dat appellant gebruik maakte van twee verzwegen bankrekeningen. Achteraf bleek dat hij met die rekeningen nooit iets te maken heeft gehad. Dat de rekeningen toch met hem in verband zijn gebracht, was te wijten aan een - door appellant blijkbaar niet verder uitgezochte - fout in het gegevenstraject tussen de bank, de Belastingdienst, het Inlichtingenbureau en de gemeente. De Centrale Raad van Beroep stelde vast dat het intrekken van bijstand bij besluit van 10 juli 2007 moet worden aangemerkt als een onrechtmatige daad jegens betrokkene, mede gelet op het feit dat dit besluit was herroepen bij besluit van 29 oktober 2007. Daarmee was volgens de Raad ook de toerekening van deze onrechtmatige daad aan het bestuursorgaan gegeven. Het bestuursorgaan oordeelde dat de schadevergoedingsplicht moest komen te vervallen gelet op art. 6:101 BW (eigen schuld). De Raad was het daarmee niet eens, maar oordeelde dat betrokkene geen hoger beroep had ingesteld tegen de afwijzing van enkele nadere schadeposten.

Het wordt niet duidelijk om welke schadeposten het hier gaat, en de rechtbank-uitspraak is niet gepubliceerd. Deze uitspraak toont echter aan dat een bestuursrechtelijke procedure tot verkrijging van schadevergoeding naar aanleiding van vernietigde besluiten zeker niet kansloos is. Dat kan mede worden verklaard door de vaste jurisprudentie van de civiele rechter dat met de vernietiging door de

bestuursrechter van een appellabel besluit, de onrechtmatigheid van dat besluit is gegeven.[54] Vaste rechtspraak is verder dat met de vernietiging ook de schuld aan de zijde van de overheid is gegeven: de toerekening van de onrechtmatigheid wordt dus eveneens verondersteld.[55] Men spreekt in dit verband wel van een ‘risicoaansprakelijkheid’ van de overheid. Wel moet ook nog aan aanvullende eisen moet worden voldaan: zo is met de onrechtmatigheid van het vernietigde besluit nog niets gezegd over het causaal verband tussen deze vernietiging en de schade en evenmin iets over de vraag of het vernietigde besluit de strekking had om de benadeelde te beschermen (de eis van relativiteit). De toepassing van deze eisen zal bij schade door onrechtmatige terugvorderingsbesluiten als regel geen problemen opwerpen. Zo wordt causaal verband geacht te ontbreken wanneer in plaats van het onrechtmatige besluit een andere besluit had kunnen worden genomen met precies dezelfde rechtsgevolgen. Bij schade door een onrechtmatig terugvorderingsbesluit van gelden die door identiteitsfraude zijn verkregen, is het niet goed voorstelbaar dat eenzelfde besluit met precies dezelfde rechtsgevolgen zal worden genomen. Aan het besluit kleeft immers een evident materieel gebrek, zodat niet bij de veronderstelde ontvanger had mogen worden teruggevorderd. Daarmee is het causaal verband tussen de schade en het onrechtmatige besluit gegeven. Voorts mag worden verondersteld dat bepalingen als de onderzoeksplicht (artikel 3:2 Awb) in deze context mede tot strekking heeft om de benadeelde te beschermen tegen de schade die hij heeft geleden doordat het bestuursorgaan heeft nagelaten de feiten zorgvuldig vast te stellen, zodat ook aan de eis van relativiteit snel zal zijn voldaan. De vraag blijft wel of de benadeelde nog schade heeft als het herstel al heeft plaatsgevonden door de bestuursrechtelijke procedure en de reactie daarop door het bestuursorgaan.

[54] HR 31 mei 1991, *NJ* 1993, 112 (*Van Gog/Nederweert*).

[55] HR 9 mei 1986, *NJ* 1987, 252 (*Van Gelder*), HR 26 september 1986, *NJ* 1987, 253 (*Hoffman La Roche*).

Overige onrechtmatige handelingen: de zoektocht naar de zorgplicht

Wordt de schade veroorzaakt door feitelijk handelen of niet appellabel bestuurshandelen, dan zal men in een civiele procedure kunnen proberen de schade vergoed te krijgen. Daarbij valt te denken aan systematische feitelijke weigeringen om onjuiste registraties te corrigeren, het op andere wijze defungeren van databanken voor gegevensopslag of feitelijke opsporingshandelingen (bij het vermoeden van strafbare feiten). Om te bepalen of de overheid aansprakelijk is, is het van belang of op de overheid de zorgplicht rust voor de gegevensopslag en -verwerking en of het niet voldoen aan die zorgplicht betekent dat de overheid de verantwoordelijkheid draagt voor de schade die ontstaat wanneer persoonlijke gegevens door kwaadwillende derden worden gebruikt.

Het gebrek aan richtinggevende rechtspraak maakt het lastig om te bepalen of een zorgplicht bestaat en zo ja, wat daarvan de exacte strekking is. Toch geven wetgeving en rechtspraak wel enige aanknopingspunten. Onzes inziens kan voor de invulling van de zorgplicht aansluiting worden gezocht bij

1) rechtspraak waarin de rechter heeft geoordeeld over de zorgplicht van civiele partijen (banken/telecombedrijven) die verantwoordelijk zijn voor het beheer van persoonsgegevens
2) wetgeving en rechtspraak over de zorgplicht op basis van de Telecommunicatiewet en de Wbp.

Ad 1. Zorgplicht voor gegevensbescherming/voorkomen identiteitsfraude

Mogelijk kan de zorgplicht die rust op private partijen ook leidend zijn voor de zorgplicht die dienaangaande op de overheid rust. Dat is enigszins speculatief, nu er geen rechtspraak is die dit steunt, maar betoogd kan worden dat het feit dat de overheid de partij is die de persoonsgegevens beheert niet zou moeten leiden tot een andere invulling van de zorgplicht.

Zorgplichten worden veelal aangenomen voor banken. Kanttekening daarbij is wel dat rekeninghouders op grond van de algemene voorwaarden van banken veelal een beperkte aansprakelijkheid hebben voor misbruik van hun rekening, mits zij aan bepaalde voorwaarden voldoen. Wanneer ze misbruik direct melden en er geen sprake is van grove nalatigheid of schuld, zal de bank over het algemeen snel compensatie toekennen. Enige relevante rechtspraak illustreert dit.

> Rechtbank Haarlem 22 juli 2009 (ECLI:NL:RBHAA:2009:BJ692) – Rabobank heeft een bijzondere zorgplicht en dient aanvragen/mutaties voldoende te administreren
>
> Bank heeft bankrekening omgezet naar gezamenlijke rekening en bankpas verstrekt aan partner, zonder medeweten van de initiële rekeninghouder (eiser). Eiser heeft nooit voor de wijziging en de verstrekking van de bankpas hoeven tekenen. Volgens de rechtbank Haarlem heeft de bank hiermee zijn zorgplicht geschonden. In principe ligt de bewijslast dat de pas zonder medeweten is verstrekt bij de eiser, maar, zo merkt de rechtbank op, zij is "in dit geval van oordeel dat de Rabobank de stelling van [eiser] onvoldoende gemotiveerd heeft betwist. Daarbij wordt in aanmerking genomen dat de Rabobank een bijzondere zorgplicht heeft die voortvloeit uit haar maatschappelijke functie en het vertrouwen dat deelnemers aan het betalingsverkeer daardoor in de bank stellen. Uit hoofde van deze zorgplicht wordt de Rabobank onder meer geacht de informatie geadministreerd te hebben omtrent de aanvraag van een (nieuwe) bankpas waarmee beschikt kan worden over de bankrekening van een cliënt. Gelet hierop kan de Rabobank ter weerlegging van de stelling van [eiser] niet volstaan met een enkele betwisting bij gebrek aan wetenschap." (rov. 4.2)

Uit Rechtbank Maastricht 10 augustus 2011, (ECLI:NL:RBMAA:2011:BR5064) blijkt dat een telecombedrijf aan zijn zorgplicht heeft voldaan als het klanten bij het aangaan van de verbintenis heeft gewezen op risico's van het gebruik van het product/de dienst (i.c. ging het om een inbraak op afstand in een telecomserver waarbij door onbekende derden voor honderden euro's naar Zimbabwe en Somalië is gebeld. Kosten komen voor rekening van de klant).

Het informeren van klanten over de risico's van misbruik speelt ook een hoofdrol in Rechtbank Rotterdam 4 juli 2012, (ECLI:NL:RBROT:2012:BX1419). Ook hier werd ingebroken in een telefooncentrale. Het systeem van KPN signaleerde echter de (enorme) toename van belgegevens en waarschuwde de klant vrijwillig. Door dit adequate optreden van KPN en door het op verschillende manieren informeren van klanten over het risico van hacken, valt KPN geen enkel verwijt te maken en dient de klant de kosten van de telefoongesprekken zelf te voldoen. De rechtbank merkt wel in haar conclusie op dat: "uit de bovengenoemde omstandigheden volgt dat KPN haar zorgplicht, zo die in dit geval al bestaat, jegens [partij 1] niet heeft geschonden. Dat was wellicht anders geweest indien KPN [partij 1] in het geheel niet of pas veel later zou hebben gewaarschuwd. Daarvan is in dit geval echter geen sprake" (rov. 7.1 slot)

> Als een bank (in de algemene voorwaarden) voldoende heeft gewaarschuwd voor de risico's van het gebruik van een betaalpas en duidelijke instructies heeft gegeven omtrent de mogelijkheden deze risico's te beperken, voldoet de bank aan zijn zorgplicht, zo blijkt uit Rechtbank Alkmaar 18 juli 2012 (ECLI:NL:RBALK:2012:BY0110, rov. 2.9).
>
> Waarschuwen voor risico's is voor de invulling van de zorgplicht dus belangrijk. Uit Gerechtshof 's-Hertogenbosch 6 november 2012, (ECLI:NL:GHSHE:2012:BY2749) volgt, tot slot, dat een bank deze waarschuwingen dient aan te passen als hem een andere wijze van fraude bekend is geworden (banken voerden gezamenlijk campagne ter waarschuwing voor 'phising'-fraude; eiser stelde dat de bank ook had moeten waarschuwen voor telefonische fraude waarbij de onbekende beller zich voordoet als medewerker van de bank. Het Hof constateerde dat de bank dat ook had gedaan, maar gaf wel ruimte aan eiser om de stelling nader te bewijzen; rov. 8.4.1, 8.4.4 en 8.4.5)

Uit de civiele rechtspraak over de bancaire en de telecomsector valt als grote lijn af te leiden dat bedrijven hun klanten/cliënten dienen voor te lichten over de (beveiligings)risico's bij het gebruik van hun product/dienst. Voor banken (en vermoedelijk ook voor de overheid) geldt een bijzondere zorgplicht vanwege diens maatschappelijke functie en het vertrouwen dat deelnemers aan het betalingsverkeer daardoor in de bank stellen. Deze overweging uit voornoemde uitspraak van de rechtbank Haarlem is interessant, nu betoogd kan worden dat een dergelijke functie eveneens toekomt aan de overheid. Als de wijze van fraude verandert en het bedrijf raakt hiervan op de hoogte, dient het ook onverwijld de voorlichting te veranderen. Ook bij opvallende mutaties, zoals een plotselinge toename van het aantal belgegevens, heeft het bedrijf de plicht de klant tijdig te informeren. Voorts houdt de zorgplicht in dat bedrijven een juiste administratie bijhouden van de bij hen ingediende aanvragen.

Ad 2. Aansluiting bij de Telecommunicatiewet en de Wbp
Een tweede bron van inspiratie voor de invulling van de zorgplicht zou kunnen worden gevonden in de Wet bescherming persoonsgegevens. Deze vraag overlapt dus gedeeltelijk met de subvraag over de specifieke basis voor aansprakelijkstelling. Uit artikel 13 Wbp kan inspiratie worden gevonden ter zake van de op zowel natuurlijke personen als rechtspersonen als op bestuursorgaan rustende verplichtingen bij het verwerken van datagegevens. Dit artikel luidt als volgt:

> *Artikel 13 Wet bescherming persoonsgegevens*
> De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

De wetgever heeft er – gelet op het tijdgebonden karakter van specifieke eisen waaraan de maatregelen zouden moeten voldoen – van afgezien om een opsomming te geven van mogelijke maatregelen, maar uit dit artikel valt in elk geval een zorgplicht af te leiden om 'passende technische en organisatorische maatregelen' uit te vaardigen om misbruik te voorkomen. Duidelijk is wel dat de maatregelen proportioneel moeten zijn. Het is dus niet noodzakelijk

om steeds de zwaarste beveiligingsmaatregelen te nemen. Wel geldt dat, naarmate de gegevens een gevoeliger karakter hebben, zwaardere eisen worden gesteld aan de beveiliging van die gegevens.[56]

Dat deze zorgplicht in bredere zin bestaat, blijkt ook uit de al eerder besproken positieve verplichtingen van artikel 8 EVRM. Uit de EHRM-zaak *I.t. Finland* van 17 juli 2008[57] volgt dat de Staat een eigen (systeem)verantwoordelijkheid heeft bij het beschermen van gevoelige en vertrouwelijke informatie. In deze zaak was informatie over de medische toestand van een medewerkster van een ziekenhuis vrijelijk toegankelijk voor haar collega's. Toen duidelijk was dat de informatie daadwerkelijk bekend was geworden onder collega's van de werkneemster, bleek niet meer na te gaan wie van haar collega's toegang heeft gehad tot haar dossier. Dit was reeds in strijd met de Finse wetgevingen gaf klaagster een mogelijkheid tot schadevergoeding. Het EHRM stelt voorop dat de bescherming van persoonlijke gegevens, en specifieke medische gegevens, van fundamenteel belang zijn voor het recht van een persoon op respect voor zijn/haar privé- en familieleven als bedoeld in artikel 8 EVRM. Volgens het Hof heeft de Staat de plicht om adequate maatregelen te treffen om elke mogelijkheid van ongeautoriseerde toegang tot dergelijke gegevens uit te sluiten. In de praktijk betekent dit dat de Staat wetgeving dient te ontwerpen waarin de bescherming van persoonsgegevens door private personen en instellingen wordt gewaarborgd. Als de Staat dit nalaat, handelt zij in strijd met artikel 8 EVRM en dus onrechtmatig.

[56] Onvoldoende beveiliging van bijvoorbeeld patiëntgegevens kan schending van art. 8 EVRM opleveren (EHRM 17 juli 2008, nr. 20511/03).

[57] EHRM 17 juli 2008 *EHCR* 2008/114 (I. t. Finland).

Ook twee bepalingen uit de Telecommunicatiewet (Tw) zijn van belang voor aanbieders van openbare elektronische communicatienetwerken en –diensten: artikel 11.3 en artikel 11a.1 Tw. Deze aanbieders dienen, zo blijkt uit artikel 11.3 Tw, maatregelen te treffen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers passende technische en organisatorische maatregelen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. De maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau dat in verhouding staat tot het desbetreffende risico. Blijkens het tweede lid omvatten deze maatregelen in elk geval:

> a. waarborgen dat slechts daartoe gemachtigd personeel voor wettelijk toegestane doeleinden toegang heeft tot de persoonsgegevens,
> b. de bescherming van opgeslagen of verzonden persoonsgegevens tegen onbedoelde of niet toegestane opslag, verwerking, toegang, verstrekking, wijziging, verlies, vernietiging, en
> c. de invoering van een veiligheidsbeleid met betrekking tot de verwerking van persoonsgegevens.

Op deze aanbieders is verder een meldplicht van toepassing voor het geval er, ondanks de genomen veiligheidsmaatregelen, toch sprake is van inbreuken op de beveiliging die nadelige gevolgen kan hebben voor de veiligheid van de persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een openbare elektronische communicatiedienst. In dergelijke gevallen zijn de aanbieders verplicht de inbreuk, onverwijld nadat zij die inbreuk hebben geconstateerd, te melden bij de ACM. Ook hier

kan een uitspraak van een rechtbank (Rb Rotterdam 8 januari 2015, ECLI:NL:RBROT:2015:22) een indruk geven van de toepassing van deze bepaling in de praktijk.

> In januari 2012 werd bekend dat een hacker had ingebroken in het netwerk van KPN. Deze hack was voor ACM aanleiding om een onderzoek in te stellen naar de wijze waarop eiseres invulling gaf aan de op haar rustende zorgplicht ten aanzien van de beveiliging van de persoonsgegevens die in haar systemen zijn opgeslagen. In dit onderzoek heeft de ACM geconstateerd dat KPN niet heeft voldaan aan de zorgplicht die op haar rust op grond van artikel 11.3 lid 1 in verbinding met artikel 11.2 Tw doordat zij onvoldoende passende, hoofdzakelijk organisatorische, maatregelen heeft getroffen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees (en gebruikers). ACM heeft KPN een bestuurlijke boete opgelegd van 364.000 euro. KPN is hiertegen opgekomen. De uitspraak gaat vooral over de vraag of ACM op een juiste wijze gebruik heeft gemaakt van zijn boetebevoegdheid; maar is ook interessant als voorbeeld voor de reikwijdte van de zorgplicht: “Nu vaststaat dat een hacker het netwerk binnen het kunnen dringen en daarbij toegang heeft kunnen hebben tot persoonsgegevens, maakt het voor de ernst van de overtreding niet uit dat de hack wellicht niet specifiek gericht was op toegang tot persoonsgegevens. Dit zou anders zijn wanneer persoonsgegevens in een afgescheiden beveiligde omgeving zouden zijn opgeslagen. Dit is niet gesteld of gebleken.” (rov. 5.3)

Bij het nalaten om de voornoemde maatregelen te nemen of bij het nemen van, naar later blijkt, onvoldoende waarborgen biedende maatregelen, kan de overheid aansprakelijk zijn.

Ad b. Schade

Een belangrijke vraag die vervolgens rijst is voor welke schade de overheid aansprakelijk is. Vaak zal de schade voortvloeien uit de daadwerkelijke gevolgen van identiteitsfraude, zoals onterechte rekeningen of onjuiste terugvorderingen/aanslagen. Die schadelijke gevolgen kunnen worden weggenomen door de betreffende rekeningen niet in te vorderen, niet over te gaan tot terugvordering etc., met andere woorden: door de nadelige gevolgen feitelijk ongedaan te maken. De vraag is of er na een feitelijke ongedaanmaking nog andere materiële schade resteert. Zoals eerder geconstateerd was de regering van mening dat bij de omgang met persoonsgegevens nadeel vaak niet in geld valt uit te drukken, maar veeleer immaterieel van aard is. Toch kan soms wel degelijk sprake zijn van materiele schade: er kan bijvoorbeeld sprake zijn van reputatieschade, die ertoe leidt dat iemand lucratieve opdrachten misloopt.

Schade ten gevolge van identiteitsfraude kan ook immaterieel van aard zijn: of die leidt tot zodanige spanning en frustratie dat van een normaal functioneren niet langer sprake is. Wanneer geen sprake is van zuiver vermogensrechtelijke gevolgen van identiteitsfraude, maar vooral van ongemak, stress en frustratie, zal het in de praktijk met name aankomen op een vergoeding van ‘ander nadeel’ ex art. 6:106 BW, ook wel ‘immateriële schade’ genoemd. Eerder kwam al ter sprake dat de regering bij de Wet persoonsregistraties buiten twijfel heeft willen stellen dat ook dit soort schade voor compensatie in aanmerking komt. Dat neemt niet weg dat de drempels voor de vergoeding van dit soort schade onder het regime van artikel 6:162 BW hoog zijn. Artikel 6:106 BW bepaalt onder meer dat dergelijke schade alleen voor vergoeding in aanmerking komt als de

aansprakelijke persoon het *oogmerk* had om immateriële schade toe te brengen. Daarvan zal niet snel sprake zijn, al is denkbaar dat aan deze voorwaarde wordt voldaan wanneer de overheid ook na langdurig aandringen van de benadeelde blijft weigeren om de nadelige gevolgen van de fraude ongedaan te maken.

Ad c. Causaliteit

Naast onrechtmatigheid, toerekening en schade dient er causaal verband bestaan tussen de schade en de schadeveroorzakende gebeurtenis. Ook hier geldt dat er nauwelijks civiele rechtspraak is die inzicht geeft in de toepassing van artikel 6:162 BW op gevallen van identiteitsfraude. Om de juridische (on)mogelijkheden om onrechtmatigheid van optreden van de overheid aan te tonen en schade van de overheid vergoed te krijgen, is er één voorbeeld bekend waarin de aansprakelijkheidsvragen expliciet aan de orde zijn gekomen, namelijk in de zaak *Kowsoleea.*[58]

De feiten in de zaak Kowsoleea zijn in het rapport van de Nationale Ombudsman van 21 oktober 2008 (NO 2008, 232) uitvoerig in kaart gebracht. Kort gezegd kreeg Kowsoleea ten onrechte een strafblad met 43 criminele antecedenten en stond hij ten onrechte geregistreerd als ongewenst vreemdeling. In 2003 werd hij bovendien geconfronteerd met een huiszoeking door de FIOD. Voor zijn reputatieschade en schade door het feitelijk mislopen van zakelijke opdrachten stelde hij de Staat aansprakelijk op grond van artikel 6:162 BW. De omvang van de gevorderde schade bedroeg 300.000 euro voor vermogensschade en 100.000 euro voor immateriële schade. De beweerde onrechtmatigheid was niet gelegen in de persoonsverwisseling maar door “onjuiste gegevens over [eiser sub 1] in de diverse registers niet, althans niet spoedig, te verwijderen, ondanks meerdere verzoeken daartoe” (vergelijk ook de hiervoor besproken zaak *Romet t. Nederland*).

Korte tijd voorafgaand aan de civiele procedure stelde de Ombudsman Kowsoleea in het gelijk. In de visie van de rechtbank leverde dit echter "niet onmiddellijk een onrechtmatige daad op aan de zijde van de Staat". In kort geding wees de civiele rechter de schadeclaim van Kowsoleea in zijn geheel af. Dit oordeel steunde met name op twee gronden:

1. Kowsoleea slaagde er in de visie van de rechtbank niet in om het causaal verband aannemelijk te maken tussen het handelen van de Staat en de schade in de vorm van misgelopen opdrachten/reputatieschade. In ro.v. 3.2 stelde de rechter vast dat het enkele feit dat hij was uitgesloten van de deelname aan een aanbesteding, nog niet betekende dat er een causaal verband bestond met de gebeurtenissen waarop de aansprakelijkheid van de Staat berustte.

   Ten aanzien van de immateriële schade was evenmin voldoende aannemelijk gemaakt dat, zo er al sprake zou zijn van reputatieschade, deze het gevolg was van gedragingen van de Staat in verband met het handelen van de politie. De gestelde gedragingen van Surinaamse politieambtenaren, door wie Kowsoleea was verhoord, kon niet aan de Staat worden toegerekend.
2. De handelingen van het regionaal politiekorps kunnen niet aan de Staat worden toegerekend. Elke politieregio heeft zijn

[58] Ktr. ’s-Gravenhage 2 maart 2009, ECLI:NL:RBSGT:2009:BH4957.

eigen rechtspersoonlijkheid. Voor zover van aansprakelijkheid sprake is, rust deze op de politieregio zelf en op de bij de regio werkzame politieambtenaren, wanneer zij in de uitoefening van hun functie schade aan derden toebrengen. Kowsoleea werd voor zijn eventuele (im)materiele schade dus verwezen naar de betreffende politieregio.

Ten aanzien van het handelen van de FIOD werd tot slot gewezen op de (beperkte) regeling ter zake van de vergoeding van schade ten gevolge van – achteraf bezien – onterechte hechtenis op basis van artikel 89-93 Wetboek van Strafvordering. Ook werd opgemerkt dat Kowsoleea ten onrechte was opgenomen in de justitiële documentatie, maar dat hij daaruit inmiddels was verwijderd. Dat hij enige tijd geen verklaring van geen bezwaar heeft kunnen verkrijgen doordat zijn vrijspraak pas twee jaar na de uitspraakdatum van een Hof-arrest in de documentatie werd ingeschreven, was wellicht nalatig van de Dienst Justitiële Informatie van de Staat, maar zorgde hooguit voor enige vertraging bij de oprichting van enige vennootschappen. Ook was niet gebleken dat de inmiddels wel opgerichte vennootschappen enige schade hadden geleden.

De rechtbank besloot met de stelling dat de door de Staat aangeboden coulancebetaling van 5.000 euro billijk was en wees zijn overige vorderingen af.

Deze zaak laat zien dat met name het bewijs van causaliteit tussen de schade en het handelen van de autoriteiten voor de gelaedeerde problematisch kan zijn. De benadeelde moet stellen en zo nodig aannemelijk maken dat het causaal verband bestaat (vgl. artikel 150 Wetboek van Rechtsvordering). Een aanvullend probleem dat daarbij kan spelen is dat in het geval van identiteitsfraude de gelaedeerde soms met het handelen van meerdere bestuursorganen te maken krijgt, zoals in het geval van Kowsoleea diverse regionale politieregio's maatregelen tegen Kowsoleea namen. Kowsoleea zou in zo'n geval moeten bewijzen welk deel van de schade aan welke politieregio kan worden toegerekend. Juist om dat bewijsprobleem te voorkomen besloot Kowsoleea de Staat aan te spreken, maar de rechter meende dat het handelen van individuele politieregio's niet aan de Staat kon worden toegerekend. Een 'ketenaansprakelijkheid', waarbij bijvoorbeeld één 'eigenaar' van een keten aangesproken kan worden voor afzonderlijke handelingen in de keten, is juridisch onbekend. Steeds zal de juiste natuurlijke of rechtspersoon in rechte moeten worden betrokken, aan wie een onrechtmatige daad kan worden toegerekend, waarmee de geleden schade in causale relatie staat.

Tussenconclusie: er zal pas worden aangenomen dat de overheid onrechtmatig heeft gehandeld wanneer zij een zorgplicht heeft geschonden. Wij hebben getracht enige zorgplichten te destilleren uit civiele rechtspraak over de wijze waarop telecombedrijven en banken met identiteitsgegevens dienen om te gaan. Ook de Telecommunicatiewet en de Wet bescherming persoonsgegevens geven een indicatie van mogelijk relevante verantwoordelijkheden van beheerders van datasystemen, welke bepalingen overigens niet alleen op overheden van toepassing zijn.
Bij civiele procedures die ertoe strekken om de overheid aansprakelijk te houden moet niet te licht worden gedacht over kansen op succes. Onrechtmatigheid wordt hier niet snel aangenomen, zeker niet wanneer men niet duidelijk kan maken welke zorgplicht de overheid niet in acht heeft genomen. Voor zover al onrechtmatigheid wordt aangenomen, zorgt het bewijs van de schade (veelal immateriële

schade) en het causaal verband tussen de schade en het overheidshandelen voor problemen. Het bewijs van causaal verband is voorts niet eenvoudig wanneer meerdere bestuursorganen bij de fraude betrokken zijn: alsdan zal elk van deze organen apart aansprakelijk moeten worden gesteld, waarbij het nog niet eenvoudig is om aan te tonen welk aandeel dat orgaan precies heeft gehad in het ontstaan van de schade, terwijl de toerekening van hun handelen aan de Staat evenmin eenvoudig is. Dit wat sombere beeld van de mogelijkheden om de overheid aansprakelijk te stellen kent één uitzondering, namelijk bij schade door onrechtmatige appellabele besluiten die mede onrechtmatig zijn verklaard vanwege potentiële identiteitsfraude. In die gevallen lijken de kansen op succes voor de burger groter, al biedt de rechtspraak hier evenmin veel voorbeelden van, en is ook in die zaken het niet eenvoudig om aannemelijk te maken dat na het herstel nog materiële of immateriële schade resteert.

B2. Het vergoeden van schade bij aansprakelijkstelling

Gelet op de bovenstaande conclusie is het ons niet mogelijk gebleken aan te geven in hoeverre schade daadwerkelijk wordt vergoed als een overheidsinstelling aansprakelijk is gesteld in verband met identiteitsfraude. Ook hier kan slechts worden verwezen naar het forfaitaire stelsel van de proceskostenvergoeding, die een slachtoffer na een succesvolle procedure kan worden toegewezen.